snapserver™
BY ADAPTEC

User Guide for Snap Server 110 and 210

www.snapserver.com

COPYRIGHT

Copyright © 2007, Adaptec, Inc. All rights reserved worldwide.

Information in this document is subject to change without notice and does not represent a commitment on the part of Adaptec or any of its subsidiaries. The software described in this document is furnished under a license agreement. The software may be used only in accordance with the terms of the license agreement. It is against the law to copy the software on any medium. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose without the express written permission of Adaptec, Inc.

TRADEMARKS

Adaptec, the Adaptec logo, Snap Server, the Snap Server logo, GuardianOS, SnapOS, Snap Disk, and StorAssure are trademarks or registered trademarks of Adaptec, Inc. in the U.S.A. and other countries.

Products mentioned herein are for identification purposes only and may be registered trademarks or trademarks of their respective companies. Windows, Windows NT, Internet Explorer, and Active Directory are registered trademarks of Microsoft Corporation. Java and Solaris, are registered trademarks of Sun Microsystems, Inc. Netscape is a registered trademark of Netscape Communications Corp. AppleShare, AppleTalk, Macintosh, and MacOS are registered trademarks of Apple Computer. BakBone and NetVault are trademarks of BakBone Software. AIX is a registered trademark of IBM Corporation. OpenView and HP-UX are trademarks or registered trademarks of Hewlett-Packard Company. BrightStor, Unicenter TNG, ARCserve, eTrust, and Unicenter are trademarks or registered trademarks of Computer Associates, Inc. Smart UPS and APC are registered trademarks of American Power Conversion Corporation. UNIX is a registered trademark of The Open Group. XFS is a trademark of Silicon Graphics, Inc. Backup Exec, VERITAS NetBackup BusinessServer, and VERITAS NetBackup DataCenter are trademarks or registered trademarks of VERITAS Software Corporation. Legato NetWorker is a trademark of Legato Systems, Inc. Linux is a registered trademark of Linus Torvalds. SCO Open Server and UnixWare are trademarks of the SCO Group. All other brand names or trademarks are the property of their respective owners.

REVISIONS

Adaptec, Inc. provides this publication “as is” without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. Adaptec and its subsidiaries reserve the right to revise this publication and to make changes in the content hereof without the obligation of Adaptec to notify any person of such revision or changes.

END USER LICENSE AGREEMENT (EULA)

FOR USE OF ADAPTEC STORAGE SOLUTIONS AND RELATED INSTALLATION UTILITIES

SNAP IP, ASSIST, AND SNAP SERVER MANAGER ("INSTALLATION UTILITIES"); THE SYSTEM SOFTWARE EMBEDDED IN THE SNAP SERVER STORAGE SOLUTION ("EMBEDDED SOFTWARE"); SOFTWARE MARKETED BY ADAPTEC OR THAT IS EMBEDDED IN OR OTHERWISE CONSTITUTES A PART OF ADAPTEC COMPUTER HARDWARE PRODUCT(S) (SOMETIMES REFERRED TO COLLECTIVELY HEREIN, TOGETHER WITH THE INSTALLATION UTILITIES AND THE EMBEDDED SOFTWARE, AS THE "LICENSED SOFTWARE"), EXCEPT WHERE EXPRESSLY PROVIDED OTHERWISE, ARE PROPRIETARY COMPUTER SOFTWARE BELONGING TO ADAPTEC, INC. OR ITS LICENSORS. UNITED STATES COPYRIGHT AND OTHER FEDERAL AND STATE LAWS AND INTERNATIONAL LAWS AND TREATIES PROTECT THE INSTALLATION UTILITIES AND EMBEDDED SOFTWARE.

USE OF THE SNAP SERVER STORAGE SOLUTION ("SERVER") OR THE INSTALLATION UTILITIES IMPLIES YOUR AGREEMENT TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. BY USING THE INSTALLATION UTILITIES OR THE SERVER, YOU ARE ENTERING INTO A BINDING CONTRACT WITH ADAPTEC, INC. IF YOU DO NOT AGREE TO BE BOUND BY THESE TERMS AND CONDITIONS, YOU MAY NOT USE THE INSTALLATION UTILITIES, THE EMBEDDED SOFTWARE, OR THE SERVER AND SHOULD PROMPTLY RETURN THIS ENTIRE PACKAGE, INCLUDING THE INSTALLATION UTILITIES AND SERVER, TO THE PLACE WHERE YOU PURCHASED IT FOR A FULL REFUND.

1. Ownership and Copyright. The Installation Utilities and Embedded Software are licensed, not sold to you, for use only as permitted by the terms and conditions of this Agreement. Adaptec reserves any rights not expressly granted to you. The Licensed Software is composed of multiple, separately written and copyrighted modular software programs. Various Licensed Software programs (the "Public Software") are copyrighted and made available under the GNU General Public License or other licenses that permit copying, modification and redistribution of source code (which licenses are referred to as "Public Licenses").

The Public Software is licensed pursuant to (i) the terms of the applicable Public License located in the related software source code file(s), and/or in its on-line documentation; and (ii) to the extent allowable under the applicable Public License. The GPL and source code are available at oss.snapserver.com. To receive a copy of the GNU General Public License, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Various Public Software programs are copyrighted by the Regents of the University of California and are derived from material licensed to the University of California by its contributors, to which the following disclaimer applies:

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

All other Licensed Software programs (the "Restricted Software") are copyrighted by Adaptec or its licensors and are licensed pursuant to all of the terms of this Agreement.

Copying of the Licensed Software, unless specifically authorized in writing by Adaptec, is prohibited by law. You may not use, copy, modify, sell, lease, sublease, or otherwise transfer the Installation Utilities or Embedded Software, or any copy or modification, in whole or in part, except as expressly provided in this Agreement.

PROVISIONS APPLICABLE TO RESTRICTED SOFTWARE ONLY (ARTICLES 2 - 7):

2. License. In consideration of the premises of this License Agreement, your payment of any applicable license fee for Restricted Software, and/or your purchase of a Snap Server that the Licensed Software accompanies, for the term of intellectual property protection inhering in the Licensed Software, Adaptec hereby grants to you a limited, personal, and non-exclusive license to install and execute ("Use") the Restricted Software solely under the terms and conditions of this Agreement and only on the Server in connection with which Adaptec originally provided such Restricted Software. You are given a non-exclusive license to use the Installation Utilities and Embedded Software in conjunction with a Server, make one copy of the Installation Utilities for archival and backup purposes only, and/or transfer your Server and copies of the Installation Utilities and the accompanying documentation to a third party provided that you provide Adaptec written notice of the transfer within 30 days after the transfer date and you do not retain any copy of the transferred software. Any such transferee's rights and obligations with respect to the transferred software and documentation are as set forth in this Agreement.

3. Reproduction of Proprietary Notices. You may not sublicense, distribute, rent, lease, lend, or otherwise convey the Restricted Software or any portion thereof to anyone, and under no circumstance may you use or allow the use of the Restricted Software in any manner other than as expressly set forth herein. Copies of the Installation Utilities must be labeled with the Adaptec copyright notice and other proprietary legends found on the original media.

4. Protection of Trade Secrets. The Licensed Software contains trade secrets, and in order to protect them, you agree that you will not reverse assemble, decompile or disassemble, or otherwise reverse engineer any portion of the Restricted Software, or permit others to do so, except as permitted by applicable law, but then only to the extent that Adaptec (and/or its licensors) is not legally entitled to exclude or limit such rights by contract. Except with respect to online documentation copied for backup or archival purposes, you may not copy any

documentation pertaining to the Licensed Software. You agree that your use and possession of the Licensed Software is permitted only in accordance with the terms and conditions of this Agreement.

5. Ownership of Restricted Software. You agree and acknowledge that, (i) Adaptec transfers no ownership interest in the Restricted Software, in the intellectual property in any Restricted Software or in any Restricted Software copy, to you under this Agreement or otherwise, (ii) Adaptec and its licensors reserve all rights not expressly granted to you hereunder, and (iii) the Restricted Software is protected by United States Copyright Law and international treaties relating to protection of copyright, and other intellectual property protection laws of the U.S. and other countries.

6. Termination. If you fail to fulfill any of your material obligations under this Agreement, Adaptec and/or its licensors may pursue all available legal remedies to enforce this Agreement, and Adaptec may, at any time after your default of this Agreement, terminate this Agreement and all licenses and rights granted to you hereunder. You agree that any Adaptec suppliers referenced in the Restricted Software are third-party beneficiaries of this Agreement, and may enforce this Agreement as it relates to their intellectual property. You further agree that, if Adaptec terminates this Agreement for your default, you will, within thirty (30) days after any such termination, deliver to Adaptec or render unusable all Restricted Software originally provided to you hereunder and any copies thereof embodied in any medium.

7. Government End Users. The Installation Utilities, Embedded Software, and accompanying documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202, Commercial Computer Software-Restricted Rights at 48 CFR 52.227-19, and FAR Section 12.212, and successor provisions thereof, as applicable. Any use modification, reproduction release, performance, display, or disclosure of the Installation Utilities or Embedded Software and accompanying documentation by the U.S. Government shall be governed solely by the terms of this Agreement and shall be prohibited except as expressly permitted by the terms of this Agreement.

PROVISIONS APPLICABLE TO RESTRICTED SOFTWARE AND, SUBJECT TO SECTION 1, TO PUBLIC SOFTWARE (ARTICLES 8 - 15):

8. Export Laws. Notwithstanding any provision of any Public License to the contrary, Adaptec shall have no duty to deliver or otherwise furnish source code of any Public Software if it cannot establish to its reasonable satisfaction that such delivery or furnishing will not violate applicable US laws and regulations. You hereby assure that you will not export or re-export any Licensed Software except in full compliance with all applicable laws, regulations, executive orders, and the like pertaining to export and/or re-export, including without limitation USA versions of the same. No Licensed Software may be exported or re-exported into (or to a national or resident of) any country to which the U.S. embargoes goods, or to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders. You agree to ascertain necessary licensing procedures and obtain required licenses before exporting or re-exporting either. You also agree to indemnify Adaptec and assume all financial responsibility for any losses it may suffer if you do not comply with this paragraph.

9. Disclaimer of Warranties. THE INSTALLATION UTILITIES AND EMBEDDED SOFTWARE ARE LICENSED "AS IS" WITHOUT WARRANTY OF ANY KIND. ADAPTEC HEREBY DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, RELATING TO THE INSTALLATION UTILITIES AND THE EMBEDDED SOFTWARE INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

10. Limitation of Liability. IN NO EVENT WILL ADAPTEC OR ITS LICENSORS' LIABILITY UNDER THIS AGREEMENT EXCEED THE PRICE THAT YOU PAID FOR THE INSTALLATION UTILITIES AND EMBEDDED SOFTWARE. FURTHERMORE, IN NO EVENT WILL ADAPTEC OR ITS LICENSORS BE LIABLE FOR ANY LOST PROFITS, LOST DATA, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR PUNITIVE DAMAGES ARISING OUT OF OR UNDER THIS AGREEMENT OR THE APPLICABLE PUBLIC LICENSE. The limitation of liability set forth in this paragraph will apply whether or not Adaptec or its licensor was advised of the possibility of the loss, liability, or damages and notwithstanding any failure of essential purpose of any limited remedy. Since some states do not allow exclusions or limitations of liability for consequential or incidental damages, this provision may not apply to you.

11. Waiver. No delay or failure of Adaptec to exercise any right under this Agreement, nor any partial exercise thereof, shall be deemed to constitute a waiver of any rights granted hereunder or at law.

12. Unlawful Provision(s). If any provision of the Agreement is held to be unenforceable for any reason, all other provisions of this Agreement shall nevertheless be deemed valid and enforceable to the fullest extent possible.

13. Applicable Law. Except with respect to any Public Software program for which the applicable Public License contains provisions expressly stating the applicable governing law (with respect to which the law so specified shall govern all aspects of such agreement, including the provisions incorporated into such Public License hereunder), the terms of this Agreement (including, to the extent allowable under the Public License, all software governed by a Public License which does not specify a governing law) will be governed by the laws of the State of California, without reference to its choice of law rules, and the United States, including U.S. Copyright laws.

14. Entire Agreement. This Agreement and all applicable Public Licenses supersede all proposals, negotiations, conversations, discussions, all other agreements, oral or written, and all past course of dealing between you and Adaptec relating to the Licensed Software or the terms of its license to you, and may only be modified in writing signed by you and Adaptec.

15. Contractor/Manufacturer. Adaptec, Inc. 691 Milpitas Blvd., Milpitas, CA 95035.

Contents

Preface **1**

Chapter 1 Installing the Snap Server **5**

Snap Server Connectors and Controls 6

Step 1: Connect Your Server to Your Network and to a Power Source 7

Step 2: Turn On Your Snap Server 8

Turning Off Your Snap Server 8

Step 3: Connect to the Server for the First Time 8

Connect Using the Server Name 9

Connect to a Snap Server Using Snap Server Manager (SSM) 10

Step 4: Configure your Server Using the Initial Setup Wizard 11

Server Name 12

Date/Time Settings 12

Changing the Administration Password 12

Reclaiming Snapshot Space 12

Server Registration 13

Locating Your Snap Server on Your Network 13

Windows Users 14

Macintosh Users 17

Connecting from the Web 18

Connecting from an NFS Mount 19

Connecting from an FTP Application 19

Chapter 2 Using Your Snap Server **21**

Using the Administration Tool 21

Connecting to the Home Page 21

The Administration Tool Interface 22

Use the Server Tab to 24

Use the Network Tab to 25

Use the Storage Tab to 27

Use the Security Tab to 28

Use the Monitor Tab to 29

Use the Maintenance Tab to 30

Using Snap Server Manager 31
Installing SSM 31
Using SSM to License Multiple Snap Servers 31
Using SSM to Manage Multiple Snap Servers 32

Chapter 3 Customizing Your Snap Server 33

Modifying Your Server Settings 33

Reclaiming Snapshot Space 34

Changing Disk Configuration 34
RAID Configuration Options 34

Creating Shares 36

Setting Up Security 37
Defining Snap Server Users 37
Assigning User Access 39
Assigning Disk Usage Quotas 40
Accessing the Snap Server with GUEST Privileges 41

Setting Up Notification via Email 42

Adding SnapExtensions 43

Setting up Data Protection Schedules 44
Scheduling Snapshots 44
Scheduling Antivirus Scans 44
Creating a Disaster Recovery Image 45

Using your Snap Server as a Print Server 45
Configuring the Printer on the Snap Server 45
Adding the Network Printer to the Client 46
Monitoring Print Jobs Using the Administration Tool 47
Pausing the Printer 47
Deleting a Printer from the Snap Server 48

Chapter 4 Assistance with Your Server 49

Phone Home Support 51

Glossary 53

Index 63

Use this guide to customize your Snap Server 110 or 210. Included are instructions to perform basic configuration of your Snap Server and an overview of the Administration Tool, which you can use to manage your server. For more detailed information about the advanced functions of the GuardianOS operating system, see the GuardianOS online Web Help or the *Snap Server Administrator Guide* on your User CD.

Audience

This guide is intended for individual users or system administrators who need to install and maintain a Snap Server 110 or 210 on their network. This guide assumes a basic understanding of file server functionality.

Notes and Cautions

This manual uses the following conventions:

Note A note presents time-saving shortcuts or ancillary information related to the main topic.

Caution A caution alerts you to potential hardware or software hazards in the configuration or operation of Snap Servers.

Document Organization

This document is organized as follows:

- **Chapter 1, Installing the Snap Server** shows you the basics of installing your Snap Server onto your network.
- **Chapter 2, Using Your Snap Server** describes the Administration Tool user interface and introduces you to the functions you can perform using the Administration Tool. It also provides an introduction to Snap Server Manager for managing your servers.
- **Chapter 3, Customizing Your Snap Server** teaches you how to set up security, to create local Snap Server users, and to customize your Snap Server.
- **Chapter 4, Assistance with Your Server** provides tips and tricks that do not appear in other chapters.
- **Glossary** provides brief definitions of terms that may be unfamiliar to you.

Typographical Conventions

This manual uses the following conventions.

Font convention	Usage
Bold	Emphasis
Italic	• Emphasis • The introduction of a new terms • Settings you select in the Administration Tool
Arial Bold	Menu commands, command buttons, and navigational links.
Arial	• **Text** that you type directly into a text field, a command line, or web page • Buttons on a keyboard
Courier Italic	A variable for which you must substitute a value
Courier Bold	Commands you enter in a command-line interface

Related Documents

Other sources of information about your Snap Servers are shown below.

Title	Description
Snap Server 110/210 Quick Start Guide	Installation and initial configuration instructions for the Snap Server 110 and Snap Server 210
Configuration and Hardware Options Guide	Detailed hardware configuration, options, and specification information about all Snap Servers
GuardianOS UI Web Help	Help for the Administration Tool installed on the Snap Server
Snap Server Administrator Guide	Detailed configuration and management information on using the GuardianOS Administration Tool.
ReadMeFirst.html	Description of Snap Server documentation
ReleaseNotes.html	Important, late-breaking information not included in other documentation

Service and Technical Support

For an immediate response to a service inquiry, use our Expert Knowledge Base System at http://www.snapserver.com/kb. Simply type in your question to view a list of possible resolutions to known issues. However, if none of the listed topics resolves your inquiry, you can forward the question to our technical support department, who will then email you a response. To obtain additional service or technical support for your Snap Server, call 1.408.934.7274.

Installing the Snap Server

Installing a Snap Server is a simple 4-step process.

Step 1: Connect the Snap Server to your network and to a power source.

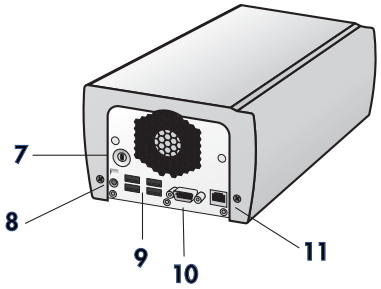
Step 2: Turn the server on.

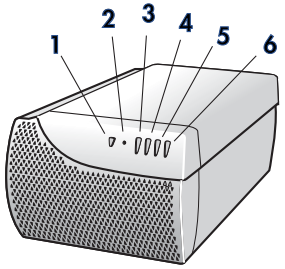
Step 3: Assign the server an IP address (if necessary) and connect to the server for the first time.

Step 4: Configure your server.

Snap Server Connectors and Controls

The Snap Server 110 and 210 have the following connectors and controls.



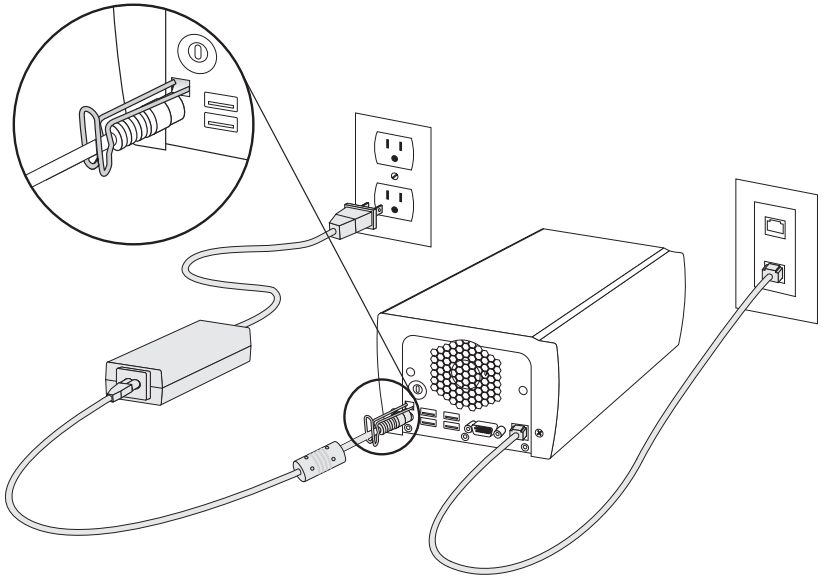


Connector/Control	Description
1 Power Button	Press the Power Button to turn the Snap Server ON and OFF.
2 Reset Button	Use the Reset Button if you cannot access the Administration Tool and you need to perform a limited reset to defaults.The Reset Button is accessed by inserting a paper clip end or small tool into the hole to the right of the Power Button when the server is fully booted and running normally.
3 Power LED	The Power LED indicates whether power to the Snap Server is ON or OFF. • **Solid green** = Server is ON • **Off** = Server is OFF
4 Status LED	The Status LED indicates whether the server is operating normally. • **Blinking green** = System is operating normally • **Blinking amber** = Thermal or other system problem
5 Network LED	The Network LED indicates whether the server is connected to the network. • **Solid green** = System is active and connected to network • **Off** = Port is disconnected or the Ethernet cable is not connected or linked to an active switch
6 Disk LED	The Disk LED indicates the status of your disk drive. • **Blinking green** = Disk drive is active • **Solid amber** = Disk drive error • **Off** = No disk drive activity

Connector/Control	Description
7 Kensington Lock Connector	The Kensington Lock slot can be used to secure a Kensington lock on your Snap Server. For more information about Kensington locks, see the Kensington Web site at www.kensington.com.
8 Power Connector	Connect your external power supply to the Power Connector. Then connect the power cord to an AC power source.
9 USB Ports (4)	Four USB ports are available for connecting an APC USB UPS, a USB printer, and a USB tape drive.
10 Service Port	The service port is for Adaptec technical support use only.
11 Ethernet Port	Connect the included Ethernet cable to the Ethernet port and then to an Ethernet outlet.

Step 1: Connect Your Server to Your Network and to a Power Source

You can connect your Snap Server to a 10BaseT, 100BaseTX, or 1000BaseT network.



1 Connect the server to your network using the Ethernet cable provided.

2 Insert the power supply retainer clip into the divets above the power connector, as illustrated in the figure above.

3 Connect the provided power supply to your Snap Server, and swing the retainer clip to fit snugly over the power connector.

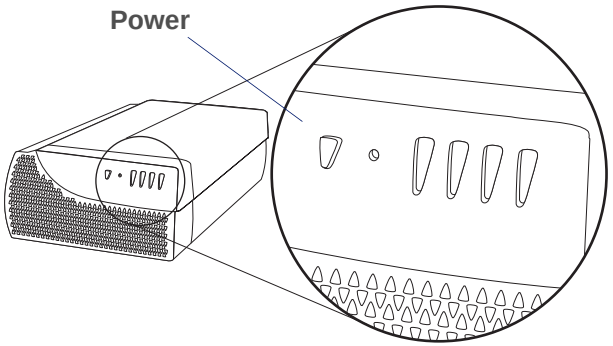
4 Connect the provided AC power cord to the power supply, then connect the server to a UPS and/or electrical outlet.

Note Your Snap Server is designed to work with an APC-brand, USB or network-based UPS device to automatically shut down cleanly in the event of an extended power failure. The APC unit must be configured in the Administration Tool and in the APC user interface. To configure the APC in the Administration Tool, go to **Server > UPS**.

Step 2: Turn On Your Snap Server

Press the Power Button until the Status light turns on, then release the button and wait for the server to start up.

When the Status light starts blinking at a steady rate (about once a second), the startup is complete.



Turning Off Your Snap Server

To turn off your Snap Server:

1 Press the Power Button until the Status light blinks three times (about one second). Release the button and wait for the lights to turn off.

2 After you turn off the Snap Server, the lights remain lit while the server completes its shutdown. You must wait for all of the lights to turn off before you turn on the server again or disconnect it from the power source. The Snap Server should never take more than thirty seconds to shut down.

Note It is important to shut down your server properly to avoid the possibility of data corruption.

Step 3: Connect to the Server for the First Time

Your Snap Server is preset to acquire an IP address automatically. If your network does not automatically assign IP addresses, you may not be able to see the server on your network and you will have to manually assign an IP address.

Two procedures are described here for connecting to the Snap Server.

Use this procedure	if...
Connect Using the Server Name	your network assigns IP addresses automatically.
Connect to a Snap Server Using Snap Server Manager (SSM)	your network does not assign IP addresses automatically or if your client cannot resolve the server name to an IP address.

Connect Using the Server Name

1 **Find the server name.**

The default server name is SNAP*nnnnnn,* where *nnnnnn* is the server number. For example, the name of a Snap Server with a server number of 401178 is SNAP401178. The server number is a unique, numeric-only string that appears on a label affixed to the underside of your Snap Server's chassis.

2 **Connect to the server.**

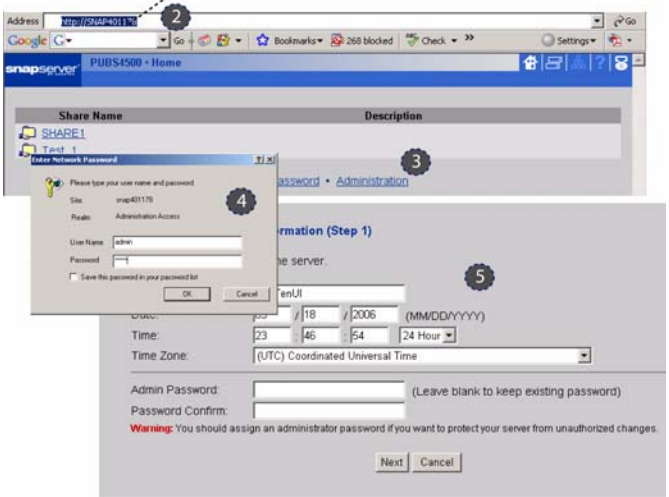
In a Web browser, enter the following URL:

**`http://SNAP`*`nnnnnn`*
(where *nnnnnn* is the server number)

3 **Press Enter.**

The Web View screen opens. Click the **Administration** link.

Note If the Web View screen does not open, perform the **Connect to a Snap Server Using Snap Server Manager** procedure.



4 **Log into the Administration Tool.**

In the login dialog box, enter *admin* as the user name and *admin* as the password, then click **OK**.

5 **Complete the Initial Setup Wizard.**

For instructions on using the Initial Setup Wizard, see page 11.

Connect to a Snap Server Using Snap Server Manager (SSM)

Use this procedure if your network does not assign IP addresses automatically or if you cannot resolve the server name to an IP address.

1 **Install SSM.**

To download and install SSM, locate the *Install_SSM.html* file on the root of your Snap Server User CD. Double-click the file to open it and follow the instructions.

Note SSM can be installed on several client platforms, including Windows, Macintosh OS X, Linux, and UNIX. If you plan to run SSM on a Macintosh client, you must upgrade the client to MacOS 10.2 or higher (required for JRE 1.4.0 or higher support).

Upon startup, SSM displays the IP address of each Snap Server on its local network segment.

2 **Launch SSM.**

Once you have installed SSM, launch it using one of the methods described in the following table:

Operating System	Procedure
Microsoft Windows 98/NT/XP/ 2000/2003/Vista	Click **Start**. Point to **Programs > Snap Server Manager**, then select Snap Server Manager.
Macintosh v10.2 or higher	Open the Snap Server Manager folder and double-click the Snap Server Manager icon.
UNIX/Linux	For default options: cd to home directory, then run the Snap Server Manager command: **`./Snap_Server_Manager`** If you selected not to create links: cd to home directory, then cd to the Snap Server Manager directory, and run the Snap Server Manager command: **`./Snap_Server_Manager`**

3 **If using a DHCP server (server that automatically assigns IP addresses), skip to the next step. Otherwise:**

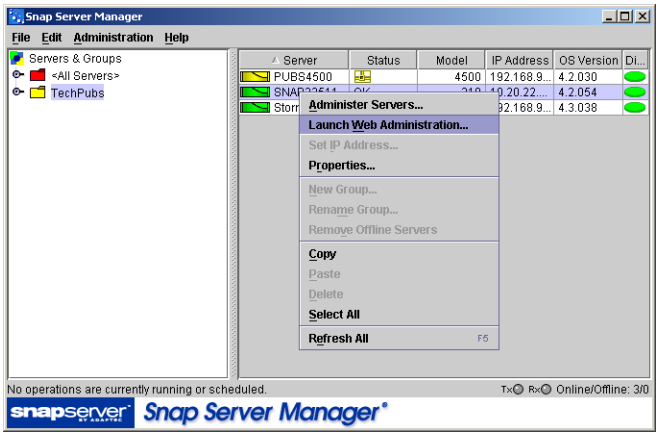
In the SSM console, right-click a server name and select **Set IP Address**. You will need to have the following information:

- The IP address for the Snap Server (required)
- The subnet mask (required)
- The default gateway IP address
- The domain server IP address
- WINS server(s) IP address(es)

At a minimum, enter an IP address for the Snap Server and a subnet mask, and then click **OK**.

4 **Launch the Administration Tool from the SSM console.**

In the SSM console, right-click a server name and select **Launch Web Administration**.



5 **Log into the Administration Tool.**

Click the **Administration** link, and in the login dialog box, enter *admin* as the user name and *admin* as the password, then click **OK**.

6 **Complete the Initial Setup Wizard.**

For instructions on using the Initial Setup Wizard, see the next section.

Step 4: Configure your Server Using the Initial Setup Wizard

The first time you connect to a Snap Server using the browser-based Administration Tool, the Initial Setup Wizard runs. The Initial Setup Wizard consists of several screens that allow you to change the server name, set the date and time, set the administrator password, configure TCP/IP settings for the Ethernet port (Ethernet1), and reclaim storage space that has been reserved in case you want to use Snapshots.

Server Name

The default server name is SNAP*nnnnnn*, where *nnnnnn* is the server number. If desired, enter a unique server name of up to 15 alphanumeric characters. In addition to letters and numbers, you can also use a dash (-) between characters, but spaces and underscores (_) are not allowed.

Date/Time Settings

The Snap Server time stamp applies when recording server activity in the event log (Monitor Menu), setting the create/modify time on a file, and when scheduling snapshot or antivirus operations. Edit the settings according to local conditions.

Note Snap Servers automatically adjust for Day Light Savings Time.

Changing the Administration Password

The default administrator user name is *admin* and the default password is also *admin*. To prevent unauthorized access to the Snap Server, enter a secure password immediately in the fields provided.

Note A password must consist of 1 to 15 alphanumeric characters and is case sensitive.

Reclaiming Snapshot Space

A Snapshot is a point-in-time image of your volume. On all Snap Servers, 20% of the default volume space is reserved in case you want to use Snapshots for backup and recovery purposes (for more information about using Snapshots, see the *Snapshots* topic in the GuardianOS online Help). The Snapshot utility must be licensed to be activated.

If you are certain that you will not use snapshots, you can reclaim that space on the volume by clicking the **Reclaim Snapshot Space** button in the Initial Setup Wizard.

Caution If you delete the snapshot space at this time (during the volume configuration process), you will not be able to restore it later if you decide that you want to use snapshots. Therefore, it is recommended that you retain the snapshot space during this initial configuration. You can always delete or reduce it from the **Storage > Snapshots** page in the Administration Tool if you have purchased a Snapshots license. Or, for servers with no Snapshots license, you can simply increase your default volume size in the **Storage > Volumes** page.

Server Registration

Register your server to receive Adaptec services and support, to create and track service requests, to download software updates, and to receive exclusive promotional offers.

To Register a Single Server

Until you register, the Registration window will appear as your opening screen every time you start the Guardian OS. Click the **Click here** link to open a separate browser window where you can register your server.

Note You can also register multiple Snap Servers in one operation using SSM. For more information, install SSM (see page 10) and refer to "Using SSM to License Multiple Snap Servers" on page 31.

Locating Your Snap Server on Your Network

Once installed on your network, the Snap Server appears as a server with a shared folder. You can use it to organize and store files in the same way that you use the folders on your local hard disk drive.

In general, you can use the following guidelines to connect to the Snap Server. These guidelines are described in more detail on the following pages.

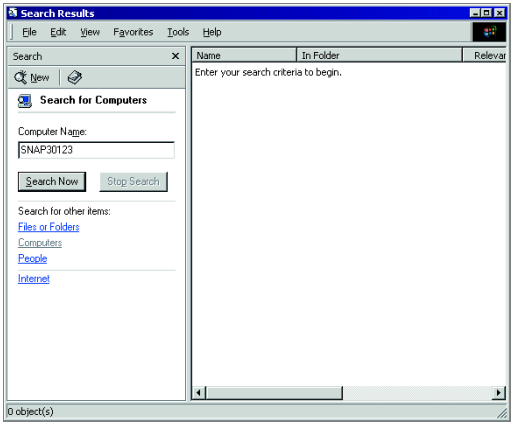
To connect to the server using:	Do this:
Microsoft Windows ®	Look for the server in **Network Neighborhood**, **My Network Places**, or **Network**. If the default settings were not changed during installation, it will appear under Workgroup.
Macintosh	Connect to the server using the **Chooser**, **Network Browser**, or **Connect to Server**.
Web browser	Enter the server name or IP address in your Web browser's location or address box.
NFS	Mount the desired share using the server name or IP address.
FTP	Enter the server name or IP address in your FTP client application.

Windows Users

Windows 2000 and Me

The Snap Server should automatically appear in My Network Places under Workgroup if the default setup was accepted during installation. If it does not appear, follow the steps described here:

1. On the Start menu, click **Search** and then **For Files or Folders**.
2. In the Search Results window, select **Computers**.
3. In the Search for Computers dialog box, enter the server name and click **Search Now**. By default your server name is based on the server number. For example, a Snap Server with the server number 30123 would by default be named SNAP30123.
4. Wait for the server to appear (you may need to try again after a few minutes if you have just turned on the server).
5. Double-click the Snap Server icon to see a folder that represents the network disk drive(s).

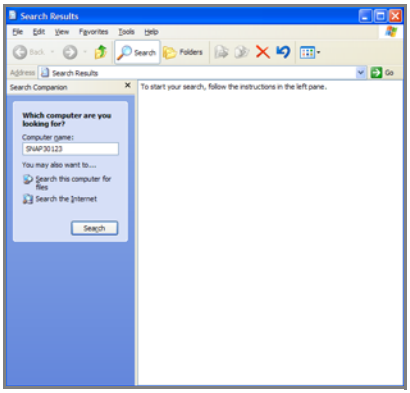


Windows XP

The Snap Server should automatically appear in My Network Places under Workgroup if the default setup was accepted during installation. If it does not appear, follow the steps described here:

1. On the Start menu, click **Search** and then **Computers or People**.
2. In What Are You Looking For, select **Computers on the Network**.

3 In the Search for Computers dialog box, enter the server name and click **Search Now**. By default your server name is based on the server number. For example, a Snap Server with the server number 30123 would by default be named SNAP30123.



4 Wait for the server to appear (you may need to try again after a few minutes if you have just turned on the server).

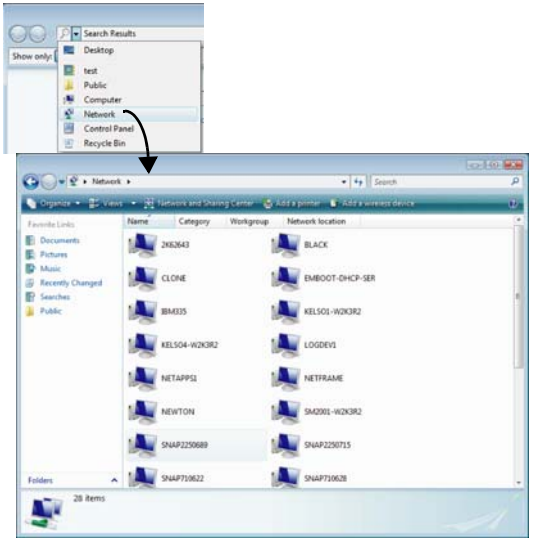
5 Double-click the Snap Server icon to see a folder that represents the network disk drive(s).

Windows Vista

The Snap Server should automatically appear in Network under Workgroup if the default setup was accepted during installation. If it does not appear, follow the steps described here:

1 On the Start menu, click **Search** and then **For Files or Folders**.

2 In the Search Results window, select **Network** in the address bar's search context drop-down menu.



Note A message may appear in the window indicating that Network Discovery is disabled. To enable it, click the message and select the appropriate icon. If Discovery is not turned on, you will not be able to see any servers on the network, though you can still connect directly to the server by mapping a network drive letter (see "Mapping a Drive in Windows" on page 16).

3 Type the server name in the Search box and press **Enter**.

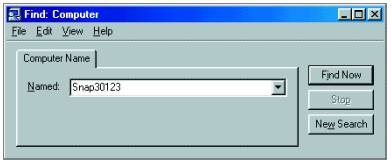
Note By default, your server name is based on the server number. For example, a Snap Server with the server number 30123 is named SNAP30123.

4 Wait for the server to appear (you may need to try again after a few minutes if you have just turned on the server).

5 Double-click the Snap Server icon to see a folder that represents the network disk drive(s).

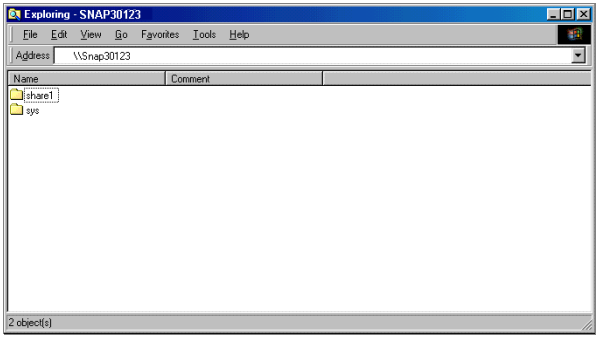
Windows 95, 98, or NT

The Snap Server should automatically appear in your Network Neighborhood under Workgroup (if the default settings were used). If it does not, follow the steps described here:



1 On the Start menu, click **Find** and then **Computer**.

2 Enter the server name. By default your server name is based on the server number. For example, a Snap Server with the server number 30123 would by default be named SNAP30123.



3 Click **Find Now** and wait for the Snap Server to appear (you may need to try again after a few minutes if you just turned on the server).

4 Double-click the Snap Server icon to see a folder that represents the network disk drive(s).

Mapping a Drive in Windows

You can also connect to your Snap Server by mapping a drive to a directory on the server. The procedure to map a drive is essentially the same for all versions of the Windows, though some of the names change slightly from version to version (e.g., My Computer in NT/2000/XP vs Computer in Vista).

1 Right-click the My Computer icon on your desktop and select **Map Network Drive**, or open Windows Explorer and select **Map Network Drive** from the Tools menu.

2 In the Map Network Drive dialog box, select a drive (or accept the default selection) and type in the Snap Server and directory you want to map using the syntax `\\server\share`. For example:

```
\\Snap401178\Share1
```

3 If you want the drive to be mapped every time you log in, click to put a check in the **Reconnect at logon** box. Click **Finish**.

4 You will be asked for your Snap Server userid and password if it is different than your Windows logon. The drive will then be visible as a network drive.

Macintosh Users

To connect to the Snap Server using MacOS 9.x

1 Select the Network Browser or Chooser from the Apple menu. In the Chooser, click the **AppleShare**® icon.

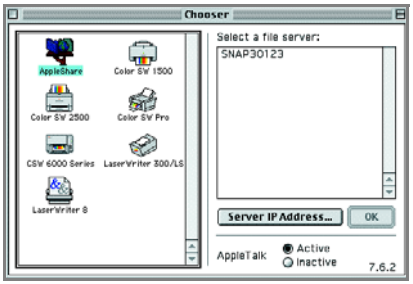
2 If you use zones with AppleTalk, select the default zone in the AppleTalk Zones® list.

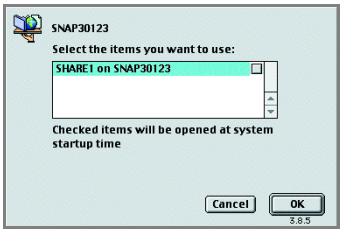
3 Scroll through the list of servers in the Select a file server list and select your Snap Server, then click **OK**.

4 When asked for a user name or password, click **GUEST**, then click **OK**.

5 In the server dialog box, select **SHARE1 on SNAP*nnnnnn***.

6 Click **OK** to mount the server on your desktop.





To connect to the Snap Server using a MacOS 10.x

1 From the Finder, click **Connect to Server** from the Go menu.

2 In the Connect to Server window, enter:

`afp://servername`

or

`afp://ipaddress`

in the Server Address box, then click **Connect**.

3 When prompted for a user name and password, enter a valid user name and password (for example, *admin*, *admin*) or click **Guest**, then click **Connect**.

4 Select SHARE1, then click **OK** to mount the server on the desktop.

To Connect to the Snap Server Using Windows Networking (SMB)

MacOS X clients who belong to a Windows domain can connect using SMB as well as Apple File Protocol (AFP).

1 Choose **Go** from the menu bar. In the Connect to Server dialog box, enter one of the following:

```
smb://servername
```

```
smb://ipaddress
```

Click **Connect**.

2 Select a share (called a volume on the Mac) to mount on your desktop.

a If "guest" is enabled for SMB or if your default log on is a valid SMB user, you will be presented with a share selection dialog box. Choose the share to connect to or click **Authenticate** to log in as a different user. A network icon should appear on your desktop for the share.

b If a user login prompt displays, enter a username and password. Once authenticated, the share selection dialog box will be displayed. Choose the share to connect to. A network icon should appear on your desktop for the share.

Note If you configured your Mac not to show drives on the desktop, you can find the Snap Server by selecting **File > New Finder Window** in the menu bar.

3 To access files on the server, double-click the icon for the share. A Finder window will display the contents of the share, and your Snap Server will now behave like any other disk on your Mac.

To disconnect from the Snap Server, drag its icon into the trash.

Connecting from the Web

By default, you can view folders and files on the Snap Server from the Web. To connect from a Web browser:

1 Type the server's name or IP address in your browser's Location or Address box.

2 Press **Enter**. This will connect you to the server's Home page.

To browse the contents of the server, click the SHARE1 link. Additional links appear if you add network shares. If you restrict access to a network share, you must log in with the right privileges to browse the contents of the share.

Connecting from an NFS Mount

To connect to the server using an NFS mount:

1. From a command line, type
   mount *server_name:/share_name /local_mount*
   where *server_name* is the name or IP address of the server, *share_name* is the name of the share to which you want to mount, and *local_mount* is the name of the mount target directory.
2. Press **Enter**. You are now connected to the specified share on the server.

For more details about working with NFS Networks, see the GuardianOS online Help or the *Administrator Guide* on your user CD.

Connecting from an FTP Application

To connect to the server using FTP:

1. Type the server's name or IP address in your FTP program's Location or Address box.

   To connect via a command line, type

   ftp *server_name*

   To connect via a Web browser, type

   ftp://*server_name*

   where *server_name* is the name or IP address of the server.
2. Press **Enter**. This connects you to the server's FTP root directory. All shares and subdirectories will appear as links or folders.

If you restrict access to a network share, you must log in with the right privileges to browse the contents of the share. You cannot manage files or folders in the FTP root directory.

For more details about working with FTP, see the GuardianOS online Help or the *Administrator Guide* on your User CD.

Using Your Snap Server

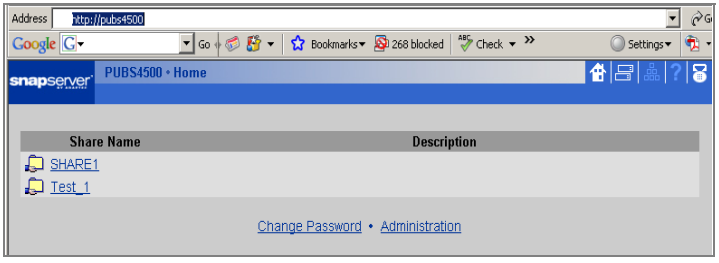
You can connect to the server with your Web browser to perform administrative tasks using the GuardianOS Administration Tool.

This chapter gives you a brief introduction to the Administration Tool interface and functionality. It does not attempt to cover all of its features. For in-depth information about the tasks you want to perform, use the GuardianOS online Help or reference the *Administrator Guide* on your User CD.

Using the Administration Tool

Connecting to the Home Page

To display the Snap Server Home page, start your Web browser, enter the server's name or IP address in the Address or Location box, and press **Enter**.

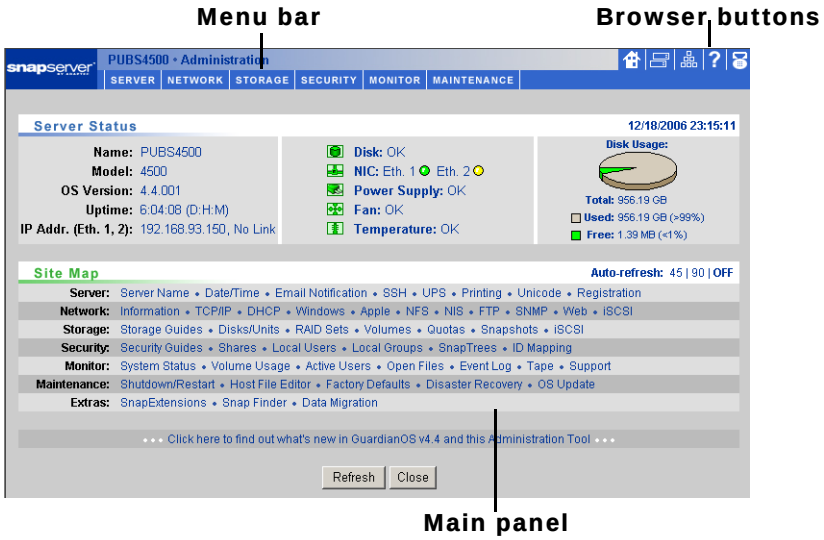


From the Home page, you can:

- Click a Share icon to access the folders and files within that share.
- Click the **Change Password** link to change the password for a local user. (Local users are described in "Defining Snap Server Users" on page 37.)
- Click the **Administration** link to log in and display the Administration menu where you can access server management features and perform administrative tasks.

The Administration Tool Interface

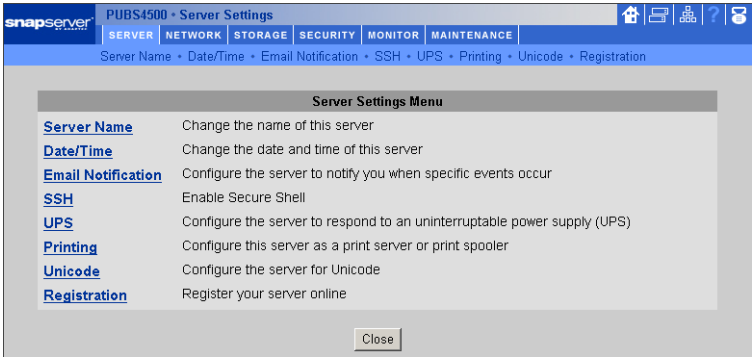
When you click the **Administration** link and log in to the Administration Tool, a screen similar to the following opens, displaying status information about your server and a site map of the different GuardianOS menus. The screen contains three major activity areas.


Menu bar
Browser buttons
snapserver
PUBS4500 • Administration
SERVER
NETWORK
STORAGE
SECURITY
MONITOR
MAINTENANCE
Server Status
12/18/2006 23:15:11
Name: PUBS4500
Model: 4500
OS Version: 4.4.001
Uptime: 6:04:08 (D:H:M)
IP Addr. (Eth. 1, 2): 192.168.93.150, No Link
Disk: OK
NIC: Eth. 1 Eth. 2
Power Supply: OK
Fan: OK
Temperature: OK
Disk Usage:
Total: 956.19 GB
Used: 956.19 GB (>99%)
Free: 1.39 MB (<1%)
Site Map
Auto-refresh: 45 | 90 | OFF
Server: Server Name • Date/Time • Email Notification • SSH • UPS • Printing • Unicode • Registration
Network: Information • TCP/IP • DHCP • Windows • Apple • NFS • NIS • FTP • SNMP • Web • iSCSI
Storage: Storage Guides • Disks/Units • RAID Sets • Volumes • Quotas • Snapshots • iSCSI
Security: Security Guides • Shares • Local Users • Local Groups • SnapTrees • ID Mapping
Monitor: System Status • Volume Usage • Active Users • Open Files • Event Log • Tape • Support
Maintenance: Shutdown/Restart • Host File Editor • Factory Defaults • Disaster Recovery • OS Update
Extras: SnapExtensions • Snap Finder • Data Migration
• • • Click here to find out what's new in GuardianOS v4.4 and this Administration Tool • • •
Refresh
Close
Main panel

Activity Area	Description
Menu bar	The menu bar displays six tabs. Click one to open the menu for that set of functions. The options will appear below the menu bar and in the screen's main panel.

Activity Area	Description	
Browser buttons		**Home—**Click to return to the Home page, which shows the server status and site map.
		Snap Finder—Click to open a screen identifying all of the Snap Servers currently on your network. You can access any of the Snap Servers by clicking the **Server Name** or **IP address** link.
		SnapExtensions—Click to open the SnapExtensions screen, where you can configure or manage licenses for third-party software.
		Help—Click to open the online help for the Administration Tool.
		Contact Us—Click to open a screen where you can access online Technical Support for your Snap Server.
Main panel	When a Menu Bar tab is selected, the functions associated with that tab are displayed in the main panel with brief descriptions of the activities you can perform by clicking that link.	

Use the Server Tab to...



- **Change server settings** — Modify the server name, date, and time.
- **Set up email notification** — Set up the server to send out email notifications when events occur (such as a server restart, server overheating, drive failure, RAID rebuild, trial license expiration, or volume space reaching limit).
- **Configure Secure Shell (SSH)** — SSH is a service that provides a remote console for special system administration and customer support access to the server. SSH is similar to telnet but more secure, providing strong encryption so that no passwords cross the network in clear text.

  Caution SSH is disabled by default, and should only be enabled to install or start a supported backup agent, or under the direction of a technical support representative. To maintain security, disable SSH immediately after the task is complete.
- **Configure UPS as your power source** — Adaptec recommends that you use an APC-brand UPS as a power source to ensure a clean shutdown in the event of an extended power failure, and to automatically restart the server when the power outage is over. Use this screen to enable UPS in the GuardianOS. You will also need to configure the UPS in the APC user interface.
- **Set your server up to be a print server** — Set your server up to be a print server for USB-connected printers.

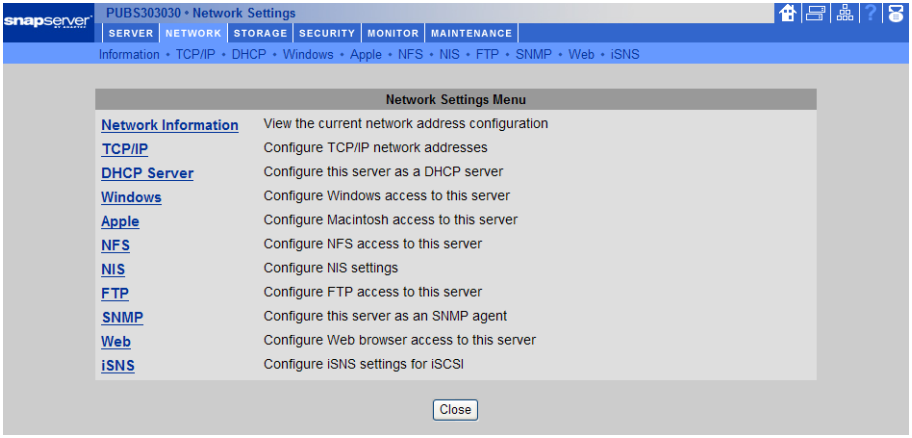
Use the Server Tab to...

- **Configure Unicode —** Unicode defines a universal means of representing characters in all languages, allowing better interoperation of varying languages using different alphabets and character sets in file and user names. More information is available at http://www.unicode.org and in the *Unicode* topic of the online Help or *Administrator Guide*.

  Caution Once Unicode has been enabled on a GuardianOS Snap Server, it is not possible to disable Unicode. Enabling Unicode will alter the functionality of some third party applications and SnapExtensions that do not fully support Unicode.

- **Register your server —** Register your server to receive Adaptec Trusted Services and support, to create and track service requests, to download software updates, and to receive exclusive promotional offers.

Use the Network Tab to...



- **View network settings for your Snap Server —** The **Network Information** link allows you to view the current network configuration.
- **Assign a static IP address —** Use the **TCP/IP** link to assign a static IP address (e.g., if your network does not automatically assign IP addresses).
- **Configure the Snap Server to be a DHCP server —** Click the **DHCP** link to enable/disable the Snap Server to be a DHCP (Dynamic Host Configuration Protocol) server and dynamically acquire IP addresses.

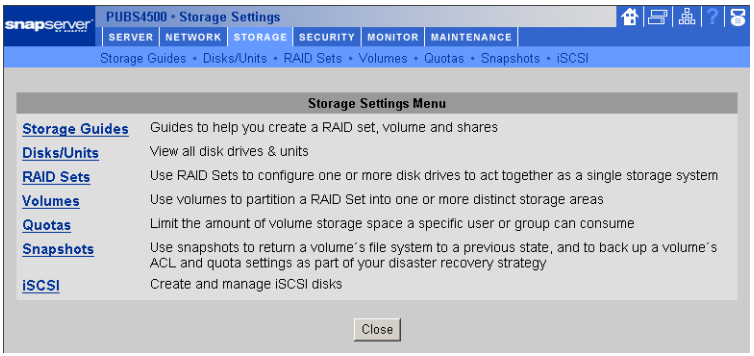
  Note To be a DHCP server, the server must have a static IP address.

Use the Network Tab to...

- **Configure access for various protocols —** The GuardianOS supports access to the Snap Server from a variety of platforms.
  - The **Windows** link configures Windows access and enables/disables the Guest User account.
  - The **Apple** link enables/disables AFP (Apple File Protocol) for Macintosh systems.
  - The **NFS** link enables/disables NFS (Network File System) for Unix and Linux users.
  - The **NIS** link configures NIS (Network Information Service), a means to manage centralized User IDs (UID) and Group IDs (GID).
- **Configure FTP access and Anonymous User Access —** The **FTP** link allows you to enable/disable FTP (File Transfer Protocol), a standard Internet protocol that provides a way to exchange files between computers on the Internet. You can also allow/disallow Anonymous Users to access your server via the web.
- **Configure the Snap Server as an SNMP agent —** Use the **SNMP** link to enable/disable SNMP (Simple NetWork Management Protocol), a system to monitor and manage network devices such as computers, routers, bridges, and hubs.
- **Configure web browser access —** The **Web** link lets you enable/disable http: access (http: is nonsecure; https: is secure), and require authentication for Web View users.
- **Configure iSNS —** If you have iSCSI disks, configure iSNS (Internet Storage Name Service) by clicking the **iSNS** link. iSNS facilitates the automated discovery, management, and configuration of iSCSI. For more information about iSCSI and iSNS, see the *iSCSI* topic in the online Help.

  Note A license is required to activate iSCSI.

Use the Storage Tab to...


snapserver
PUBS4500 • Storage Settings
SERVER
NETWORK
STORAGE
SECURITY
MONITOR
MAINTENANCE
Storage Guides • Disks/Units • RAID Sets • Volumes • Quotas • Snapshots • iSCSI
Storage Settings Menu
Storage Guides
Guides to help you create a RAID set, volume and shares
Disks/Units
View all disk drives & units
RAID Sets
Use RAID Sets to configure one or more disk drives to act together as a single storage system
Volumes
Use volumes to partition a RAID Set into one or more distinct storage areas
Quotas
Limit the amount of volume storage space a specific user or group can consume
Snapshots
Use snapshots to return a volume's file system to a previous state, and to back up a volume's ACL and quota settings as part of your disaster recovery strategy
iSCSI
Create and manage iSCSI disks
Close

- **Create RAID Sets, Volumes, and Shares —** The **Storage Guides** link opens the RAID wizard, which takes you through the steps to create or modify a RAID, volumes, and shares.

  You can also create or modify your RAID by clicking the **RAID Sets** link. And you can create or modify volumes using the **Volumes** link.

  See page 34 for more information about modifying your disk configuration.

- **View your disk drive information —** The **Disks/Units** link opens a page that displays a graphic representation of disk status and the RAID configuration on your server.

- **Assign Quotas —** The **Quotas** link opens a page where you can set limits to the amount of space different users have available on the volume. For more information about assigning quotas, see page 40.

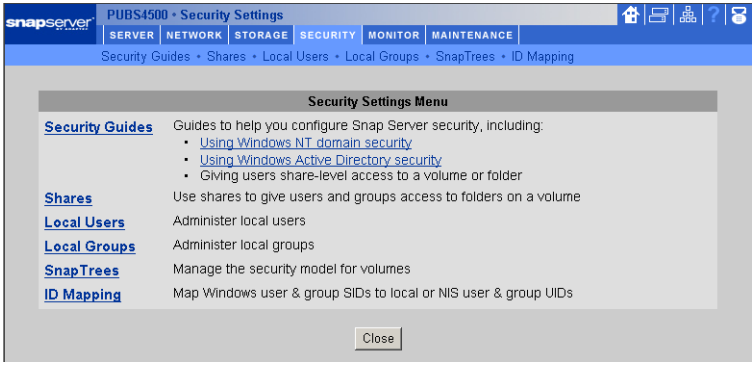
- **Schedule a Snapshot —** The **Snapshots** link opens a page where you can schedule a snapshot of your volume to be used for backup or recovery purposes. For more information about Snapshots, see page 34.

  Note Snapshots require a separate license (available through the SnapExtensions page), and space allotted on the volume (see page 34 for more information).

- **Create or modify an iSCSI disk —** Use the **iSCSI** link to create or modify an iSCSI disk. For more information about iSCSI, see the *iSCSI* topic in the online help.

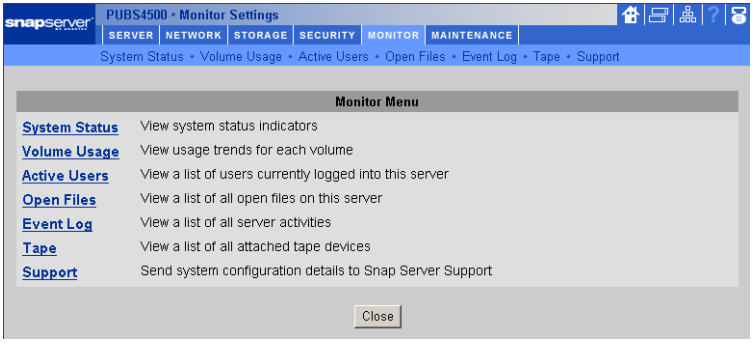
  Note iSCSI requires a separate license (available through SnapExtensions).

Use the Security Tab to...


snapserver
PUBS4500 • Security Settings
SERVER
NETWORK
STORAGE
SECURITY
MONITOR
MAINTENANCE
Security Guides • Shares • Local Users • Local Groups • SnapTrees • ID Mapping
Security Settings Menu
Security Guides
Guides to help you configure Snap Server security, including:
Using Windows NT domain security
Using Windows Active Directory security
Giving users share-level access to a volume or folder
Shares
Use shares to give users and groups access to folders on a volume
Local Users
Administer local users
Local Groups
Administer local groups
SnapTrees
Manage the security model for volumes
ID Mapping
Map Windows user & group SIDs to local or NIS user & group UIDs
Close

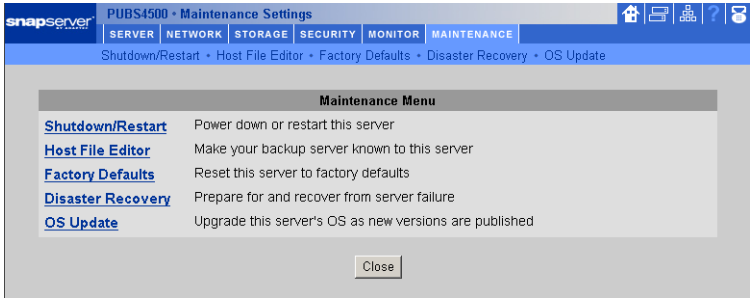
- **Configure Windows network access —** The **Security Guides** link takes you through the steps to automatically add your Windows network users to the Snap Server user list. See page 37 for more information.
- **Create or modify shares —** The **Shares** link opens a page where you can create or modify shares on your volume. You can then apply rules to allow or restrict users from accessing the shares.
- **Create or modify users and groups —** The **Local Users** and **Local Groups** links open pages where you can create users and groups on the Snap Server, and you can specify their access privileges.
- **Assign a security model to your volume —** The **SnapTrees** link opens a page where you can assign either a Windows- or a UNIX-style security model to the volume. The security model determines the file-level security scheme that will apply to files and folders within the volume or SnapTree directory. New volumes default to the Windows-style security model.
- **Map IDs between Windows and local or NIS users —** The **ID Mapping** link opens a page where you can map IDs, allowing users and groups that exist on Windows domains to share user IDs with local or NIS users and groups. This results in the same permissions and quota consumption applying to both the Windows domain user and the local or NIS user.

Use the Monitor Tab to...



- **View system configuration and user information —** From the Monitor tab, you can view the following:
  - System status information, including server name, model, OS version, server number, CPU, memory, etc. (**System Status**)
  - The amount of space remaining on your volume(s) (**Volume Usage**)
  - The number of users who are logged into the Snap Server (**Active Users**)
  - The number of open files on the server (**Open Files**)
  - A list of server activities, including errors, warnings, and other information (**Event Log**)
  - A list of USB tape backup devices attached to the server (**Tape**)
- **Send system information to Adaptec —** Click the **Support** link to open a page where you can send your system information to Adaptec technical support for troubleshooting.

Use the Maintenance Tab to...

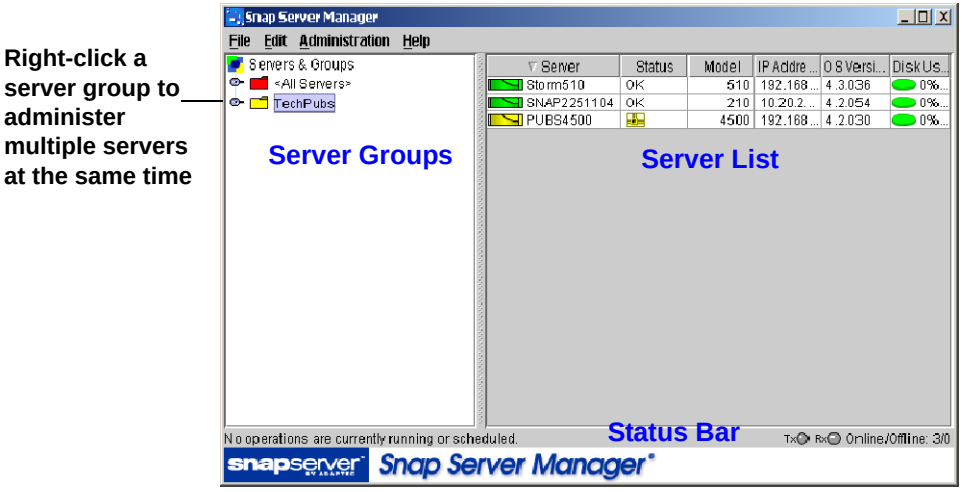


- **Shut down or restart your server** — Click the **Shuddown/Restart** link to open a page where you can gracefully (safely) shut down or restart your server.
- **Identify backup or media servers** — Click the **Host File Editor** link to supply a hostname-to-ip address mapping that identifies backup or media servers in the Snap Server's hosts file.
- **Reset your server to factory defaults** — Click the **Factory Defaults** link to reset your server settings (network configuration, system settings, access settings) to the factory defaults.
- **Create a recovery image** — Click the **Disaster Recovery** link to open a page where you can create a recovery image of the server volume, select to recover server-specific settings, or select to recover volume-specific settings.
- **Update your GuardianOS** — Click the **OS Update** to open a page where you can download and install the latest GuardianOS update from the Snap Server web site.

Using Snap Server Manager

You can manage your Snap Servers using Snap Server Manager (SSM), a java-based, platform-independent utility that allows you to discover, configure, and monitor all of the Snap Servers on your network. You can also compare, copy, and configure settings for groups of GuardianOS Snap Servers in a single operation.

Note Managing multiple servers using Snap Server Manager requires a separate license for each additional server you wish to manage.



Installing SSM

To install and launch SSM, follow the instructions in "Connect to a Snap Server Using Snap Server Manager (SSM)" on page 10.

Using SSM to License Multiple Snap Servers

You are automatically licensed to use SSM with a single server at a time. However, if you use SSM to manage multiple servers, you must purchase a license for each server. Registering your Snap Servers first will streamline the license acquisition process.

1 **Purchase a license for each Snap Server.**

Visit the Snap Server web site (http://www.snapserver.com) and navigate to the Snap Server Manager page to purchase an SSM license for each Snap Server. You will receive an email containing proof of purchase (PoP) numbers that you can use to generate your SSM licenses.

2 **In SSM, access the License Required dialog box.**

With PoP numbers at hand, start SSM and select the servers to be licensed. Then select the **Administration > License Servers for SSM** command and enter the necessary administrative password(s). The License Required dialog box opens.

3 **Generate the license keys using the Snap Server Registration Server.**

In the License Required dialog box, click the **Obtain license keys** link to open the Registration Server page. If you have already registered your servers, the fields for the server and serial numbers you need to generate the keys will automatically populate. Complete the remainder of the required fields as indicated on the page and then submit the form to obtain the license keys.

Note Should you need to enter the serial number manually, you can find the number (a 10-character alphanumeric string) on a label affixed to the underside of your Snap Server.

4 **Copy and paste the license keys into SSM's Enter License dialog box.**

Copy the license keys from the page generated by the Registration Server. Then, in the License Required dialog box, click **Enter License**, paste the keys in the space provided, and then click **OK**. The licensed state should now read *licensed*.

Using SSM to Manage Multiple Snap Servers

If you have more than one Snap Server on your network, you can use SSM to manage them all at the same time.

Some of the multiserver management features include:

- **Simultaneous application of settings to server groups —** You can organize GuardianOS servers into functional groups and apply settings to all servers in the group simultaneously.
- **Comparing settings across servers —** SSM can compare settings across any number of GuardianOS servers and identify when settings differ among servers. For example, comparing protocol access configuration for a group of servers may reveal that settings are consistent for Windows, NFS, and AFP but that differences exist among servers in HTTP/HTTPS and FTP settings.
- **Copying settings from one server to one or more different servers —** SSM can copy selected settings (TCP/IP, SNMP, SMB, etc.) from any GuardianOS server to one or more different GuardianOS servers.
- **Scheduling operations to run during offpeak hours —** Operations can be scheduled to run on multiple GuardianOS servers during offpeak hours.
- **Automatic email notification of completed operations —** You can configure SSM to send an operations report (CSV format) upon completion of any operation.

Customizing Your Snap Server

Your Snap Server is configured so that you can use it immediately in its default condition. Or, you can also customize the server to your own specifications.

Customizations can include:

- Modifying your server settings
- Reclaiming snapshot space
- Changing the default storage configuration
- Creating Shares
- Setting up security by assigning file access permissions and quotas to users

  Caution By default, no security restrictions are in place for accessing the files and folders within the Snap Server. Anyone who can connect to the Snap Server from your network or from the Internet can access any of the server's files. If you are concerned about the security of your files, you will want to set up users and access restrictions.
- Enabling email notification
- Enabling third party software
- Setting up data protection schedules
- Configuring your server to be a print server

Modifying Your Server Settings

When you first set up your Snap Server, the Initial Setup Wizard guides you through configuring the server name, date and time, login name, and password. You can change these settings at any time by starting the Administration Tool and selecting the **Server** tab, then selecting the setting you want to modify (see "Using Your Snap Server" on page 21 for an introduction to using the GuardianOS Administration Tool).

Reclaiming Snapshot Space

A *Snapshot* is a single point-in-time image that is taken of a volume. It can then be used to back up the volume without interfering with activity on the live volume. In the event of corruption, it can also be used to restore the volume or files on the volume to the snapshot state. All Snap Servers are configured with 20% of the default volume set aside for snapshots.

Note Snapshot capability is built into your Snap Server system, but it must be licensed before it can be used. To license Snapshots, click the SnapExtensions icon in the upper corner of the Administration Tool screen, then click the License Required link next to Snapshots.

The Initial Setup Wizard prompts whether you want to continue to reserve 20% of disk space for future snapshot use. If you choose to preserve Snapshot space and later decide that you do not plan to use snapshots or you want to change the amount of space set aside, you can modify or remove the space allotted by going to **Storage > Volumes**, clicking the volume, then changing the volume size.

Changing Disk Configuration

Your Snap Server's disk configuration was preset at the factory, and the default disk settings depend on the Snap Server.

Caution Make changes to the disk configuration before you store any files on the server. Changing the configuration will erase all data stored on the disk drives.

RAID Configuration Options

Snap Server 110

The Snap Server 110 has a single disk, which supports only a 1-drive RAID 0 configuration.

Because a single disk can only support RAID 0, you cannot change the RAID level. However, you can change the number and/or size of the volumes on the RAID if you wish to create separate file systems. The Snap Server ships with a single default volume. You can delete the default volume and create multiple smaller volumes on

the RAID if desired. However, be aware that deleting the default volume may also disable some third party applications that reside on the volume.

Note Before reconfiguring the volume space, be sure to review the *Volumes* topic in the Admnistration Tool's online Help.

To modify your RAID configuration, navigate to **Storage > Storage Guides** in the Administration Tool. The RAID wizard will step you through the process of making volume and share modifications.

Snap Server 210

The two-disk Snap Server 210 has three RAID configuration options:

- RAID 0 (2-drive stripe, single large volume): The two disk drives are combined into one larger disk, and data is striped across the disks. This is the default configuration. It provides the best performance but does not provide data protection.
- RAID 0 JBOD (two independent volumes): Each of the two disk drives is configured as a 1-drive RAID 0.
- RAID 1: One disk duplicates the data stored on the other disk. This configuration is also known as disk mirroring. You only have half your storage space available for data using this configuration, but, if a disk fails, the remaining disk automatically takes over and the server continues operating without interruption or loss of data.

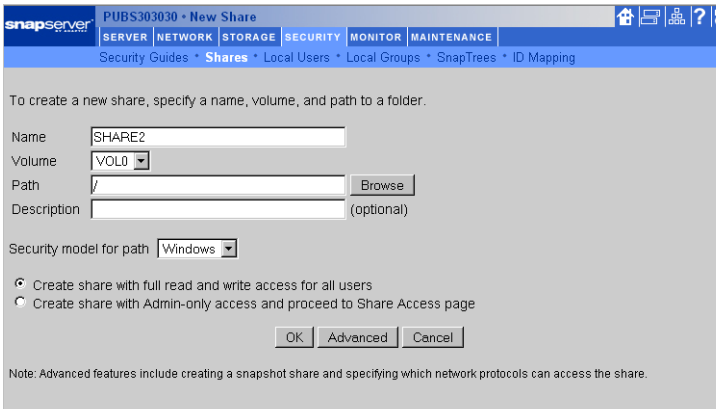
To change disk settings, navigate to **Storage > Storage Guides** in the Administration Tool and select the type of RAID you want to configure.

snapserver
PUBS4500 • Administration
SERVER
NETWORK
STORAGE
SECURITY
MONITOR
MAINTENANCE
Storage Guides • Disks/Units • RAID Sets • Volumes • Quotas • Snapshots • iSCSI
There are currently 2 disks available for configuration. Please select the type of RAID set you wish to create.
One Large Disk (RAID 0 / Stripe)
Combine two or more disks to make one large RAID set (no redundancy).
Data Protection (RAID 1 / Mirror)
Two or more disks can automatically back up a single disk.
Close

The RAID wizard will step you through the process of configuring the RAID, volumes, and shares.

Note Before reconfiguring volume space, be sure to review the *Volumes* topic in the Admnistration Tool's online help.

Creating Shares



Your Snap Server is pre-configured with one volume (VOL0) and one share (SHARE1). You can use this configuration and simply add subdirectories, folders, and files to the default SHARE1, or you can create new shares if your environment requires a more complex configuration (e.g., you want to restrict access to or hide certain shares). To create a new share, navigate to **Security > Shares** in the Administration Tool and click **New**. Provide the required name, location, and security model information about the new share. Click the **Advanced** button to specify hidden shares, network access, or Snapshot shares. For detailed information about creating and configuring a share, see the WebUI Online Help.

Setting Up Security

snapserver
PUBS4500 • Security Settings
SERVER
NETWORK
STORAGE
SECURITY
MONITOR
MAINTENANCE
Security Guides • Shares • Local Users • Local Groups • SnapTrees • ID Mapping
Security Settings Menu
Security Guides
Guides to help you configure Snap Server security, including:
Using Windows NT domain security
Using Windows Active Directory security
Giving users share-level access to a volume or folder
Shares
Use shares to give users and groups access to folders on a volume
Local Users
Administer local users
Local Groups
Administer local groups
SnapTrees
Manage the security model for volumes
ID Mapping
Map Windows user & group SIDs to local or NIS user & group UIDs
Close

To control who can access the files and folders stored on the server, you must set up security restrictions. To set up security on your server, use the settings on the **Security** menu in the Administration Tool.

Caution The default configuration allows all users on your network full access to all disks on the server. If you have Web access enabled, this could include Internet users as well, depending on your network setup. If you intend to store sensitive data, you should define tighter security restrictions before putting the data on the server.

Setting up security for the files and folders on your Snap Server consists of the following three steps:

1. **Define the Snap Server users**
2. **Assign user access**
3. **Assign disk usage quotas**

Defining Snap Server Users

Before you can give or deny access to a server, you need to identify the users. The Snap Server by default provides a set of pre-defined users and groups. Your server also allows you to use pre-existing Network Users or to define Local Users and Groups.

Pre-defined Users and Groups

Snap Servers ship with the following predefined local users and groups that allow administrative and guest user access to the server. These local users and groups cannot be modified or deleted.

Default Local Users and Groups	
admin	The *admin* user account is used to log into the Administration Tool. The default password for the admin account is also *admin*.
guest	The *guest* user account requires no password.

Default Local Users and Groups	
AllLocalUsers	The *AllLocalUsers* group account includes all local users created on the Snap Server.
AllUsers	The *AllUsers* group account includes all local, Windows domain, and NIS users.
admingrp	The *admingrp* account includes the default admin user account. Any local user accounts created with admin rights are also automatically added to this group.

Defining Network Users

Network Users are users whose information the server obtains from a Microsoft Windows domain. These network services allow you to define users in a central location and use those definitions across your network.

To access network user lists, click **Security > Security Guides**, then do one of the following:

- Click **Using Windows NT domain security** to add Microsoft Windows NT network users that are part of the domain. Read the initial screen, then click **Next** to continue. You are guided step-by-step to add desired users.
- Click **Using Windows Active Directory security** to add Microsoft Windows Active Directory (ADS) domain users. Read the initial screen, then click **Next** to continue. You are guided step-by-step to add desired users.

Defining Local Users

Local Users are users you define on a specific Snap Server. All of their user information is stored on the server.

To simplify user access for Windows Workgroup or Macintosh clients, create local accounts on the Snap Server that match those used to log into client workstations. This strategy allows users to bypass the login procedure when accessing the Snap Server.

To define Local Users, click **Security > Local Users**, then click **New**. You can use other buttons on this page to manage Local Users.

Defining User Groups

You can define *User Groups* and you can also give or deny access to the entire group. If you have defined network users, any groups defined in the Microsoft Windows domain service are available for you to use on the server.

To define groups of Local Users, click **Security > Local Groups**, then click **New**. You can use the other buttons on the Security page to manage local user groups.

Assigning User Access

Access to Network Shares

Network shares are virtual folders that map to an actual directory on the server. They are equivalent to Microsoft networking shares, Macintosh networking shared folders, and NFS exported file systems.

Snap Servers are configured at the factory with one share for the default volume and RAID. You can create additional shares that represent an entire disk or a folder within a disk by clicking **Security > Shares**, then clicking **New**.

You can also assign users or groups access permissions (full access, read only, or access denied) to shares. These access permissions apply to all files and folders accessible through the share.

To assign access permissions:

1. Click **Security > Security Guides.**
2. Click the **Give users share-level access to an entire volume** or **Give users share-level access to a folder on a volume**.
3. Follow the instructions to select or create a share, and to give or restrict access to that share.

Access to Files and Folders

If desired, you can assign the following access permissions to specific files and folders on your Snap Server:

Full Access	User/group has full access privileges.
Read Only	User/group can only read the contents of the files or folders.

For example, you may have a network share open for full access by EVERYONE. You can prevent certain files (or folders) from being overwritten by changing their access rights from "Full Access" to "Read Only." You can also control access to individual files (or folders) by adding users (or groups) with specific rights to the list of who can access the files (or folders).

To assign access permissions to a share:

1. Select **Security > Shares** in the Administration Tool. The server displays a list of network shares that you have defined.
2. Highlight the share to which you want to assign permissions and click the **Access** button.
3. Select the users and groups you wish to add, pick the appropriate security level, and click **Add** to add them to the security list. To change the access permissions

for a user (or group), select the user or group whose access you wish to modify, select the new permissions level from the drop down list, click the **Change Access** button, then click **OK**.

To assign access permissions to files and folders within a share (Windows NT, 2000, and XP):

1. In Windows Explorer, right-click the folder or file to which you want to assign permissions, select **Properties**, and select the **Security** tab.
2. Add or remove users and groups, and assign permissions to each.
3. If you want this folder automatically to inherit the permissions of the parent folder, select the **Advanced** button and click to place a check in the **Allow inheritable permissions from parent to propagate to this object** box.
4. Click **OK** to save your changes.

To assign access permissions to files and folders within a share (Windows Vista):

1. In Windows Explorer, right-click the folder or file to which you want to assign permissions, select **Properties**, and select the **Security** tab.
2. Click the **Edit** button, then add or remove users and groups, and assign permissions to each. When you have finished, click **OK**.
3. If you want this folder automatically to inherit the permissions of the parent folder, return to the Security tab, select the **Advanced** button, click **Edit**, and click to place a check in the **Allow inheritable permissions from this object's parent** box.
4. Click **OK** to save your changes.

The access permissions you assign to specific files and folders work in conjunction with access permissions you assign to a network share. When access rights for a user or group to a share differ from those to a file or folder in the share, the most restrictive access right is enforced. For more information about the method used by the GuardianOS to restrict access rights, review the *Share and File Access* topic in the online Help.

Assigning Disk Usage Quotas

If desired, you can control how much disk storage space a user can use on the Snap Server.

For example, you may want to prevent some of your users from using more than 100 MB of disk space each, but you may also want to allow other users to operate without any restrictions.

To assign disk usage quotas:

1. Navigate to **Storage > Quotas** in the Administration Tool. If the **Enabled** link is **Yes**, continue to the next step. If the link is **No**, click the link, then click to put a check in the **Enable Quotas on Volume [xxxx]** box. You can also define a default quota from this screen.
2. Click the volume on which you want to assign quotas. The server displays a list of users along with their current disk space allocation and consumption.
3. Select the user for whom you want to assign a quota.
4. Enter the amount of disk space you want that user to have, or choose the No Limit selection if you want the user to have no quota. Click **OK**.

If you have enabled the Snap Server email notification feature (see "Setting Up Notification via Email" on page 42), the server informs you whenever users fill up their available disk space.

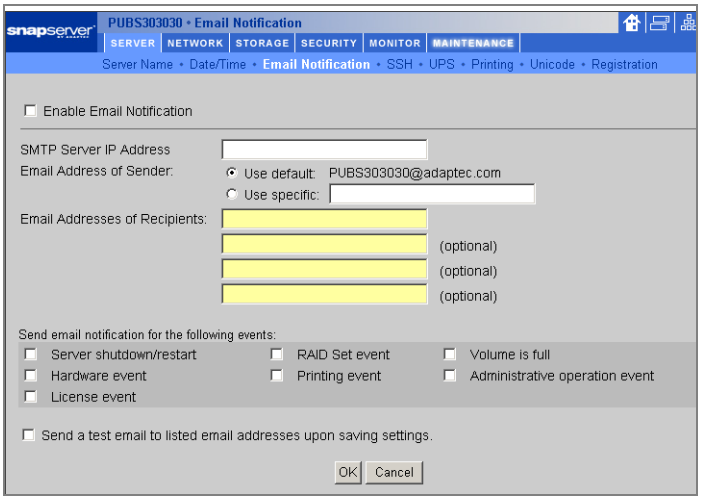
Accessing the Snap Server with GUEST Privileges

By default, a Snap Server has a predefined local user named GUEST that, if enabled, allows anyone to use the Snap Server. If a user tries to access the Snap Server and is not recognized or if the user connects as an anonymous user via FTP, then that user is identified as GUEST and has whatever access privileges that have been allowed to GUEST, AllLocalUsers, and/or AllUsers. Depending on the level of security you require, you may want to restrict GUEST privileges when accessing some (or all) network shares.

Setting Up Notification via Email

When certain events occur, an email notification can be sent to the administrator. To configure this feature, do the following:

1. From the Administration Tool, select **Server > Email Notification**.
2. Click to put a check in the **Enable Email Notification** box.
3. Fill in the IP Address of the server, the email address of the sender, and the email addresses of people you want to receive the notifications.
4. Put checks in the boxes of all events you want to trigger email notifications, and click **OK**.



Note You may want to send a test email to confirm your settings. Check the **Send a test email...** box to do so.

Adding SnapExtensions

SnapExtensions are software applications, agents, and utilities that extend the capabilities of a Snap Server. Some SnapExtensions are fully functional out-of-the-box; others may require a download and/or the purchase of a license for full operation. For up-to-date information on feature availability, contact Adaptec.

Note Licenses can be obtained by clicking the **License required** link next to the specific item on the SnapExtensions screen.

To access SnapExtensions, click the SnapExtensions icon from any page in the Admnistration Tool.

Feature	Description
CA eTrust Antivirus	Preinstalled antivirus software that requires a license to activate. For more information about CA eTrust Antivirus, see the online Help.
BakBone NetVault	Preinstalled backup software that requires a license to activate. For information on installing and configuring NetVault, see the documentation included with the NetVault CD that shipped with your Snap Server.
NDMP (Network Data Management Protocol) Server	Preinstalled NDMP agent that allows the Snap Server to participate in NDMP-based backup solutions. To enable the service, a license is required.
Snap EDR Agent	Utility included with your Snap Server that moves, copies, or replicates the contents of a share from one Snap Server to another share on one or more different Snap Servers. Comes with a 45-day trial license, but requires a license for each Snap Server thereafter.
Snap Server Manager	Pre-installed utility for managing multiple Snap Servers simultaneously. Functional out-of-the-box for single-server administration; but a license is required for multiserver administration. For more information, see “Using Snap Server Manager” on page 31.

Feature	Description
iSCSI	*Internet SCSI* (or iSCSI) is an iSCSI disk located on a Snap Server volume which appears to a client machine as a local SCSI drive. This storage virtualization frees the administrator from the physical limitations of direct-attached storage media on network clients or servers, allowing capacity to be expanded easily as needed. A separate license is required.
Snapshots	A snapshot is a consistent, stable, point-in-time image of a volume that can be backed up independent of activity on the live volume. Snapshots can also satisfy short-term backup situations such as recovering a file deleted in error, or even restoring an entire file system, without restoring from tape. A separate license is required to activate Snapshots.

Setting up Data Protection Schedules

Note Additional licenses are required to activate Snapshots and CA Antivirus.

Scheduling snapshots and antivirus scans, and creating a disaster recovery image preserves your server configuration and protects your data from loss or corruption.

Scheduling Snapshots

Navigate to **Storage > Snapshots** to schedule snapshots or modify the space available for storing snapshots. Snapshots should be taken when the system is idle or under low data traffic. For more information about scheduling snapshots, see the *Snaphots* topic in the Administration Tool online Help or the *Administrator Guide* on your User CD.

Scheduling Antivirus Scans

To enable antivirus protection:

1. Click the **SnapExtensions** icon, then click **CA Antivirus**.
2. Click the checkbox to enable antivirus, then click **OK**. The browser will take you back to the SnapExtensions screen.
3. Click **CA Antivirus** again and click the configuration link to launch the *e*Trust administration user interface for configuration and scheduling of virus scans and virus signature file updates.

For more infomation about scheduling antivirus scans, see the *CA eTrust Antivirus Software* topic in the Administration Tool's online Help or the *Administrator Guide* on your User CD.

Creating a Disaster Recovery Image

Create a disaster recovery image (DRImage) on the **Maintenance > Disaster Recovery** page. This DRImage should be created after the server configuration is complete, and can be used to recover the server or a replacement server to the configured state. Review the *Disaster Recovery* topic in the online Help for more detailed information.

Using your Snap Server as a Print Server

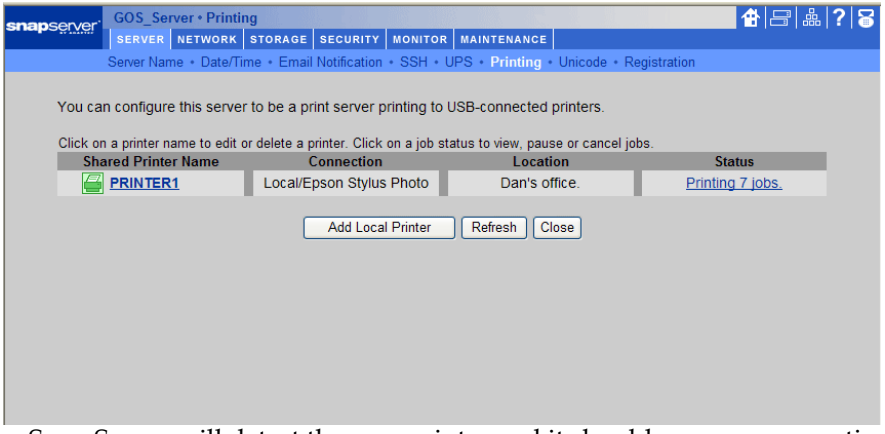
The Snap Server can be configured to emulate a Windows print server for up to four locally-attached USB printers. Client machines connect to the Snap Server over the network and share the printers. You can pause or resume the printer, and monitor or cancel print jobs using the Administration Tool.

Configuring your Snap Server as a print server is a two part process.

- First configure the printer on the Snap Server.
- Next configure the client to print via the Snap Server.

Configuring the Printer on the Snap Server

1. Connect the printer to one of the USB ports on the Snap Server.
2. Power on the printer.
3. In the Snap Server's Administration Tool, navigate to **Server > Printing**. A list of currently defined USB printers is displayed. To add the new printer, click **Add Local Printer**.



4. The Snap Server will detect the new printer and it should appear as an option in the **Local Printer Device** dropdown list. Select that printer.

5 Give the printer a name, and complete Desciption and Location information as desired. Click **OK**. The printer will appear in the list on the main printing page.

Adding the Network Printer to the Client

The Snap Server supports both Windows SMB (SAMBA) and IPP printing protocols.

Note To make printer drivers easily accessible to users, copy them to a share which everyone can access on the Snap Server.

Adding the NetWork Printer to a Windows Client

Windows offers several methods for adding a printer. Follow your usual method. When asked to locate the printer, if you are using SMB, enter the Snap Server name or IP address; if you are using IPP, enter the exact path as follows in the URL field:

`http://`*`servername`*`:631/printers/`*`sharename`*

where *servername* is the name or IP address of your Snap Server and *sharename* is the name of the printer.

Note 631 is the IPP port number.

If you experience difficulty adding the printer, try the following:

1 Navigate to **Start > Run** and enter the server name as follows:
servername

2 After a delay, you may be prompted for a user name and password. Log in as a user with access to the Snap Server.

3 A Windows Explorer window will open displaying all shares and printers on the server. Right-click the server and choose **Connect**.

Adding the Network Printer to a Mac OS X Client

Add a printer using your usual method. If you are using SMB, you will need to know the Snap Server name. If you are using IPP, you will need to enter the IP address in the **Type** field and the printer and sharename in the **Queue** field.

Adding the Network Printer to a Linux Client

Add a printer using your usual method. If you are using SMB, you will need to know the Snap Server name. If you are using IPP, enter the exact path as follows in the URL field:

`http://servername:631/printers/sharename`

where *servername* is the name or IP address of your Snap Server and *sharename* is the name of the printer.

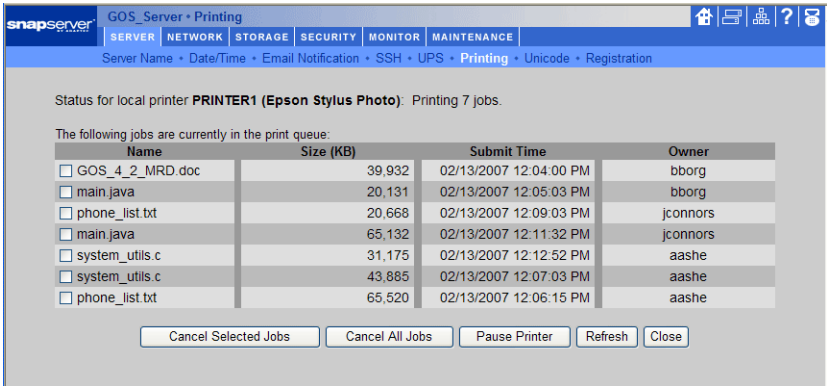
Note 631 is the IPP port number.

Monitoring Print Jobs Using the Administration Tool

Pause or resume the printer, and check the status of or cancel print jobs from the Snap Server's Administration Tool.

To Cancel Print Jobs

1 Navigate to **Server > Printing** and click the Status link next to your printer to open the Job Status window and see your print job queue.



2 To cancel a print job, click to put a check in the box next to the job you want to remove and click **Cancel Selected Jobs**. You can select to cancel multiple jobs. If you want to cancel all the listed print jobs, click the **Cancel All Jobs** button. Click the **Refresh** button to update the screen with the current list of print jobs.

Pausing the Printer

Click the **Pause Printer** button to pause all print jobs. When the printer is paused, the button will become a **Resume Printer** button, which you can click to resume printing.

Deleting a Printer from the Snap Server

When you remove a printer, remember to remove its information from both the Administration Tool and the client machines.

1. Disconnect the printer cable from the Snap Server.
2. In the Administration Tool, navigate to **Server > Printing**. In the list of printers, the status of printer you just removed should appear as Offline.
3. Click the printer link to open the Edit Printer page, then click the **Delete** button to delete the printer.

Assistance with Your Server

This chapter contains answers to several frequently asked questions. For more troubleshooting tips, visit the Snap Server Web site at http://www.snapserver.com/support.

Question:	Answer:
Can I use standard UNIX file security on my Snap Server?	Yes. GuardianOS supports standard UNIX-type file security. However, you should configure SnapTrees in order to get proper support. For information about configuring SnapTrees, see the *SnapTrees and Security Models* topic under *Share and File Access* in the GuardianOS online Help or the *Administrator Guide* on your User CD.
Can I use a third-party utility to defragment Snap Server hard disks?	No. Snap Servers use XFS, which is highly efficient in preventing file fragmentation when hard disks are not filled to greater than 90% of their capacity.
How can I back up a Snap Server?	The Snap Server can be backed up over the network from a workstation or remote server with a backup device such as a tape drive or hard drive connected to the workstation or remote server. For information on the currently supported backup applications, see the *Third Party Backup Applications* topic in the GuardianOS online Help.
How can I back up my system settings?	In addition to backing up the data stored on the Snap Server, you may also back up its system and volume settings. The **Maintenance > Disaster Recovery** screen allows you to create the files you need to restore these settings
How do I grant complete access to a few users on my network, but not others?	The simplest way is to use the browser-based security setup screen to enter the user names of the people you want to allow access to the Snap Server. Then either remove or password-protect the GUEST user account. Users defined in the Snap Server's security automatically become members of the EVERYONE group, which is granted complete access to all shares in the default configuration. By disabling or password protecting the GUEST account, you prevent connection by any user not defined to the Snap Server's security. See “Accessing the Snap Server with GUEST Privileges” on page 41.

Question:	Answer:
How do I reset my server to factory defaults?	Open the Administration Tool, and navigate to **Maintenance > Factory Defaults**. Select from: • Reset Network Configuration to Factory Defaults • Reset System Settings, Network and Admin Passwords to Factory Defaults • Reset to default ACLs for volume: xxxx Select the desired settings and click **OK** to restore default settings.
How do I reset Snap Server settings if I cannot connect to it?	Resetting the Snap Server to its factory default settings does not change the existing disk configuration or erase any data stored on your disks. While the server is running and fully booted, push the reset button with a paperclip. The server will reboot and perform a limited reset to defaults, including the following: • Clears user-defined settings such as DHCP configuration • Resets the server name to its default setting (SNAP<server number>) • Resets network speed and bonding settings to their defaults • Resets the Administrator password to the default (admin) • Resets the web server to allow http
Why does Windows sometimes inaccurately report free space?	Some Windows clients are unable to recognize free disk space in excess of 2GB. This problem only affects the display, it does not affect the available space or your ability to use it. Use a Web browser to determine how much free space is actually available.

Phone Home Support

Once your Snap Server has been registered, Phone Home Support becomes available for use. Phone Home Support emails system logs and files that contain information useful for troubleshooting purposes to Adaptec technical support. You can use the **Monitor > Support** screen to open a new case with technical support; or, in the course of working to resolve an issue, a technical support representative may ask you to fill out and submit this page. If a case is already in progress, you will need to enter the case number provided by the technical support representative.

Notes Phone Home Support interacts with two fields on the **Server > Email Notification** screen: (1) To use Phone Home Support, you must enter a valid SMTP server IP address on the Email Notification screen; and (2) the first email address listed in the Recipient(s) field populates the Admin Email Address field on the Support screen.

Complete the following fields as appropriate, then click **OK**:

Text Field	Description
Subject	(Required) Enter a concise description that identifies the issue.
Case	(Required) Select *New Case* if you are emailing technical support for the first time. Select *Existing Case* if you have previously contacted technical support concerning the issue.
Case Number	If you selected *Existing Case* above, enter the case number provided by technical support.
Reply-to Address	(Required) This field defaults to the first email address entered as a recipient on the **System > Email Notification** screen. If necessary, enter at least one email address that will serve as the contact email address for this issue. To receive a copy of the email and system information attachment, select the *Cc Admin* check box.
Comments	(Required) Enter additional information that will assist in the resolution of the problem.

Glossary

Term	Definition
access permissions	A rule associated with a share, a file, or a directory to regulate which users can have access to the share and in what manner.
ACL (Access Control List)	The list that controls access to directories and files. Each ACL includes a set of access control entries, which contain the metadata that the system uses to determine access parameters for specified users and groups.
Administration Tool	A Web-based utility used for configuration and ongoing maintenance, such as monitoring server conditions, configuring email alerts for key events, or for SNMP management.
AFP (AppleTalk Filing Protocol)	A Local Area Network (LAN) architecture built into all Apple Macintosh computers.
agent	A program that performs some information-gathering or processing task in the background. Snap Servers support Data Protection Agents and can be configured as SNMP agents.
AllLocalUsers group	The default group for all local users on Snap Servers. Local users are set up by the Snap Server administrator. Network users or Windows domain users are not part of the AllLocalUsers group.
AllUsers group	A collection of all users. The Snap Server automatically maintains the AllUsers group.
array	A series of objects, all of which are the same size and type. In a server context, an array refers to the grouping of hard drives into a RAID set.
authentication	The validation of a user's identity by requiring the user to provide a registered login name and corresponding password.

Term	Definition
autonegotiation	An Ethernet feature that automatically negotiates the fastest Ethernet speed and duplex setting between a port and a hub or switch. This is the default setting and is recommended.
autosensing	An Ethernet feature that automatically senses the current Ethernet speed setting.
CA *e*Trust Antivirus	The antivirus software bundled with the Snap Server.
CIFS (Common Internet File System)	The default Windows protocol for communication between computers. A specification for an Internet file access protocol that complements HTTP and FTP and reduces access time.
default gateway	The router used when there is otherwise no known route to a given subnet.
degraded	A RAID state caused by the failure or removal of a disk drive in which data is consistent, but there is no redundancy.
DHCP (Dynamic Host Configuration Protocol)	A communications protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a computer network. Each system that connects to the Internet/intranet needs a unique IP address. The Snap Server can be configured to perform as a DHCP server and assign IP addresses with a single subnet.
directory	A virtual folder used to organize files. Also called a folder.
disaster recovery	A strategy that allows a company to return to normal activities after a catastrophic interruption. Through failover to a parallel system or by restoration of the failed system, disaster recovery restores the system to its normal operating mode.
disk	A rigid platter, usually constructed of aluminum or mylar, with a magnetic surface that allows the recording of data, that is stored inside the drive.
DNS server (Domain Name System server)	The server that maintains a mapping of all host names and IP addresses. Normally, this mapping is maintained by the system administrator, but some servers support dynamic mappings.
domain	A set of network resources in Windows NT and Windows 2000/2003/XP/Vista, such as users and groups of users. A domain may also include multiple servers on the network. To gain access to these network resources, the user logs into the domain.

Term	Definition
domain name	The ASCII name that identifies the domain for a group of computers within a network.
Ethernet	The most widely installed LAN technology. 100Base-T Ethernet provides transmission speeds of up to 100 Mbps. Fast Ethernet or 1000Base-T provides transmission speeds up to 1000 Mbps and is typically used for LAN backbone systems, supporting workstations with 100Base-T cards. Gigabit Ethernet (GbE) provides an even higher level of backbone support at 1000 Mbps (one Gigabit or one billion bits per second).
Ethernet address	The unique six-digit hexadecimal (0-9, A-F) number that identifies the Ethernet interface.
Ethernet port	The port that houses the network card to provide Ethernet access to the computer.
event	Any significant occurrence in the system that may require notifying a system administrator or adding an entry to a log.
FTP (File Transfer Protocol)	A standard Internet protocol that provides a way to exchange files between computers on the Internet. By default, a Snap Server is set up to be an FTP server.
GID (group IDs)	On a Snap Server, the unique ID assigned to each group for security purposes.
GuardianOSImage.gsu	An image file used to upgrade the GuardianOS.
hidden share	A share that restricts the display of the share via the Windows (SMB), Web View (HTTP/HTTPS), FTP, and AFP protocols.
host name	The unique name by which a computer is known on a network. It is used to identify the computer in electronic information interchange.
HTTP (Hypertext Transfer Protocol)	An application protocol for transferring files (text, graphic images, sound, video, and other multimedia files) over TCP/IP on the World Wide Web.
HTTPS (Hypertext Transfer Protocol Secure)	The HTTP protocol using a Secure Sockets Layer (SSL). SSL provides data encryption, server authentication, message integrity, and client authentication for any TCP/IP connection.
I/O (Input/Output)	The operation of transferring data to or from a device, typically through an interface protocol like CIFS, NFS, or HTTP. The Snap Server presents a file system to the user and handles block I/O internally to a RAID array.

Term	Definition
Inheritance	In Windows permissions, inheritance is the concept that when permissions for a folder are defined, any subfolders within the defined folder inherit its permissions. This means an administrator need not assign permissions for subfolders as long as identical permissions are desired. Inheritance greatly reduces administrative overhead and also results in greater consistency in access permission management.
IP (Internet Protocol) address	The unique 32-bit value that identifies the location of the server. This address consists of a network address, optional subnetwork address, and host address. It displays as four addresses ranging from 1 to 255 separated by periods.
iSCSI (Internet SCSI)	iSCSI is a standard that defines the encapsulation of SCSI packets in TCP and then routes it using IP. It allows block-level storage data to be transported over widely used IP networks.
IPP (Internet Printing Protocol)	IPP is a printing protocol that uses HTTP. As a result, print requests can travel over your company's intranet or over the Internet
JBOD (Just a Bunch of Disks)	Disks that are left as independent volumes, not configured into a RAID array.
JVM (Java Virtual Machine)	Software that converts Java bytecode into machine language and executes it. A JVM allows an application such as Snap Server Manager written in Java to run on any operating system.
LED (Light-Emitting Diode)	An electronic device that lights up when electricity is passed through it.
Linux	A UNIX-like operating system that was designed to provide personal computer users a free or very low-cost operating system comparable to traditional and usually more expensive UNIX systems. The GuardianOS is based on the Linux operating system.
local group/local user	A group/user defined locally on a Snap Server using the Administration Tool. The local user is defined by the server administrator. Windows domain, ADS, and NIS users are not considered local.
mirroring	Used in RAID 1, a process of storing data on one disk and copying it to one or more disks, creating a redundant storage solution. RAID 1 is the most secure method of storing mission-critical data.
mounted	A file system that is available.

Term	Definition
NAS (Network Attached Storage)	Hard disk storage that is set up with its own network address as opposed to being attached to the department computer that is serving applications to a network's workstation users. By removing storage access and its management from the department server, both application programming and files can be served faster because they are not competing for the same processor resources. The NAS device is attached to a local area network (typically an Ethernet network) and assigned an IP address.
NDMP	Network Data Management Protocol, a protocol that defines a common architecture for the way heterogeneous file servers on a network are backed up. The protocol will allow the creation of a common agent used by the central back-up application to back up different file servers running different platforms and platform versions. With NDMP, network congestion is minimized because the data path and control path are separated. Back up can occur locally—from file servers direct to tape drives, while management can occur from a central location.
NetVault for GuardianOS	A comprehensive backup solution that is preinstalled on Snap Servers running GuardianOS 2.6 or higher to support backup and restore operations to a local tape drive.
NFS (Network File System)	A client/server application that allows a computer user to view and optionally store and update files on a remote computer as though they were on the user's own computer. The user's system needs to have an NFS client and the other computer needs the NFS server. The Snap Server is configured as an NFS server by default.
NIS (Network Information Service)	A network naming and administration system for smaller networks that was developed by Sun Microsystems. NIS+ is a later version that provides additional security and other facilities. The Snap Server accepts NIS users and groups.
node	Any device, including servers, workstations, or tape devices, that are connected to a network; also the point where devices are connected.
NVDB (NetVault Database) directory	A NetVault for GuardianOS database directory stored on the Snap Server that holds records for the media and backups performed.
Permissions	A security category, such as no access, read-only, or read-write, that determines what operations a user or group can perform on folders or files.

Term	Definition
PoP (Proof of Purchase)	The number used to obtain a license key for an upgrade to third-party applications.
POSIX (Portable Operating System Interface)	A set of standard operating system interfaces based on the UNIX operating system. The need for standardization arose because enterprises using computers wanted to develop programs that could run on multiple platforms without the need to recode. The Snap Server uses Extended POSIX ACLs.
protocol	A standardized set of rules that specifies the format, timing, sequencing, and/or error checking for data transmissions.
public access share	A share that allows all users read/write access to the file system.
quota	A limit on the amount of storage space on a volume that a specific user or NIS group can consume.
RAID (Redundant Array of Independent Disks)	A collection of disk drives that act together as a single storage system. Different RAID types provide different levels of data protection.
RAID 0 (Striped)	Distributes data evenly among all disks in the array. This technique, called data striping, results in fast access speeds because it uses multiple physical devices to store the data. However, RAID 0 offers no redundancy and does not accept hot spares. If a single disk drive fails, every file in the RAID is rendered unavailable.
RAID 1 (Mirrored)	Stores data on one disk drive and copies it to another drive in the RAID. A RAID 1 must contain at least two disk drives: one for the data space and one for redundancy. Although the data space in a RAID 1 can never be larger than a single drive, some administrators prefer to add a third drive (either as a hot spare or a member) for additional redundancy. RAID 1 is the most secure method for storing mission-critical data because there is no catastrophic data loss when a disk fails. However, RAID 1 is the most expensive and least efficient storage method.
recurring snapshot	A snapshot that runs at an administrator-specified time and interval.

Term	Definition
restrict anonymous	A Windows feature in which anonymous users cannot list domain user names and enumerate share names. Microsoft has provided a mechanism in the Registry called restrict anonymous for administrators to restrict the ability for anonymous logon users (also known as NULL session connections) to list account names and enumerate share names. The implementation of the restrict anonymous mechanism may prevent the Snap Server from obtaining the list of account names it needs to authenticate Windows domain users.
rollback	A snapshot feature that allows the administrator to restore a volume to a previous state as archived in a snapshot without resorting to tape.
SCSI (Small Computer System Interface)	A parallel interface standard used to attach peripheral devices, such as robotic libraries, to computers.
serial number	The ten-character alphanumeric number assigned by the manufacturer at the factory.
server number	A numeric derived from the MAC address of your Snap Server's primary Ethernet port that is used to uniquely identify a Snap Server.
share	A virtual folder that maps to the root of a volume or a directory on the volume. Permissions are assigned to a share that determine access for specific users and groups.
share access	Permissions granted or denied to users and groups that control user and group access to the files.
SMB (Server Message Block)	A protocol for Windows clients. SMB uses the TCP/IP protocol. It is viewed as a complement to the existing Internet application protocols such as FTP and HTTP. With SMB, you can access local server files, obtain read-write privileges to local server files, share files with other clients, and restore connections automatically if the network fails.
Snap EDR	A utiltiy that copies the contents of a share from one Snap server to another share on one or more Snap Servers. Snap EDR is designed to work with Snap Servers and other Snap Server Storage Solutions.

Term	Definition
Snap Server Manager (SSM)	A Java-based utility for discovering and monitoring Snap Servers.
SnapDRImage	The Snap Server disaster recovery image that saves server-specific settings such as server name, network, RAID, volume and share configuration, local user and group lists, and snapshot schedules.
SnapExtension	A Java application that extends a Snap Server's functionality. SnapExtensions are produced both by Adaptec and third-party vendors.
snapshot	A consistent, stable, point-in-time image of a volume (file system) used for backup purposes.
snapshot pool	Disk space reserved within a RAID for the storage of snapshot data. In the default storage configuration of many Snap Servers, twenty percent of the RAID capacity is allocated to the snapshot pool.
snapshot share	A virtual folder that allows access to all current snapshots at the same directory level as the original share on which it is based.
SnapTree Directory	A directory residing in the root of a volume that is assigned a Windows- or UNIX-style security model. The security model determines the file-level security scheme that will apply to files, folders, and subdirectories within the SnapTree directory.
SNMP (Simple Network Management Protocol)	A system to monitor and manage network devices such as computers, routers, bridges, and hubs. SNMP views a network as a collection of cooperating, communicating devices, consisting of managers and agents.
SSH (secure shell)	A service that provides a remote console for special system administration and customer support access to the server. SSH is similar to telnet but more secure, providing strong encryption so that no passwords cross the network in clear text.
SSL (Secure Sockets Layer)	A technology that provides data encryption, server authentication, message integrity, and client authentication for any TCP/IP connection.

Term	Definition
static IP address	An IP address defined by the system administrator rather than by an automated system, such as DHCP. The Snap Server allows administrators to use DHCP-assigned or statically assigned IP addresses.
striping	A RAID storage technique that distributes data evenly among all disks in the array.
subnet mask	A portion of a network that shares a common address component. On TCP/IP networks, subnets are all devices with IP addresses that have the same prefix.
TCP/IP (Transmission Control Protocol/Internet Protocol)	A commonly used networking protocol that supports the interconnection of different network operating systems.
trap	A signal from the Snap Server informing an SNMP management program that an event has occurred.
UI (User Interface)	The User Interface is the graphical and textual presentation of the GuardianOS in your web browser.
UID (User IDs)	A unique ID assigned to each user on a Snap Server for security purposes.
UNC (Universal Naming Convention)	In a network, a way to identify a shared file in a computer without having to specify (or know) the storage device it is on. In the Windows OS, the UNC name format is as follows: *server_name**share_name**path**file_name*
UPS (Uninterruptable Power Supply)	A device that allows a computer to keep running for a short time when the primary power source is lost. It also provides protection from power surges. A UPS device contains a battery that starts when the device senses a loss of power from the primary source.
URL (Uniform Resource Locator)	A Web address.
volume	A logical partition of a RAID's storage space that contains a file system. In the default storage configuration of many Snap Servers, eighty percent of the RAID capacity is allocated to the default volume.
Web View	The Web-browser screen that opens when users access a Snap Server using their Web browsers, and displays a list of all shares.

Term	Definition
Windows domain authentication	Windows-based networks use a domain controller to store user credentials. The domain controller can validate all authentication requests on behalf of other systems in the domain. The domain controller can also generate encrypted challenges to test the validity of user credentials. Other systems use encrypted challenges to respond to CIFS/SMB clients that request access to a share.
WINS (Windows Internet Naming Service)	The server that locates network resources in a TCP/IP-based Windows network by automatically configuring and maintaining the name and IP address mapping tables.
workgroup	A collection of computers that are grouped for sharing resources such as data and peripherals over a LAN. Each workgroup is identified by a unique name.

Numerics

1000BaseTX 7
100Base-TX 7
10Base-T 7

A

Access 26, 28, 49
- Anonymous user 26
- Apple 26
- File-level 39
- FTP 26
- Full access 39
- NFS 26
- NIS 26
- No access 39
- Privileges needed 19
- Read-only access 39
- User access 39
- Web browser 26

Active Users 29
Administration Password 12
Administration Tool 9
- Browser buttons 23
- Home page 21
- Interface 21
- Maintenance tab 30
- Menu bar 22
- Monitor tab 29
- Network tab 25
- Security tab 28
- Server tab 24
- Storage tab 27

Anonymous User 26

B

Backing Up
- Server 49
- System settings 49

BakBone NetVault 43
Browser Buttons 23

C

CA eTrust Antivirus 43
- Scheduling Scans 44

Chooser (Macintosh) 13
Connecting to a Snap Server
- FTP Users 19
- Macintosh Systems 17
- Mapping a Drive in Windows 16
- NFS Users 19
- Web Users 18
- Windows Users 14

Connectors
Ethernet port 7
Kensington Lock 7
Power connector 7
Service port 7
USB ports 7
Controls
Disk LED 6
Network LED 6
Power button 6
Power LED 6
Reset button 6
Status LED 6

D

Data Protection 44
Date/Time Settings 12
Defragmenting Snap Servers 49
DHCP 11, 25
Disaster Recovery 30
Scheduling 45
Disk Configuration
Changing 34
Snap Server 110 options 34
Snap Server 210 options 35
Disk Drive Information 27
Disk LED 6
Disk Mirroring 35
disk quotas, ***see Quotas***
Disk Striping 35
Disks/Units 27
DRImage 45
Dynamic IP Address 25

E

Email Notification 24, 42
Ethernet Cable 7
Ethernet Port 7
Event Log 29

F

Factory Defaults 30, 50
FTP 26
FTP, connecting with 13

G

Groups
Access to files and folders 39
Defining user groups 38
Pre-defined 37
GUEST 41, 49
Guest (Macintosh) 17

H

Host File Editor 30

I

ID Mapping 28
Initial Setup Wizard 10, 11
Changing the Administration password 12
Configure Date/Time settings 12
Configure server name 12
Reclaiming snapshot space 12
Server registration 13

IP Address 25
Assign Automatically 9
Assign manually 9
Using SSM to discover 10
IPP port number 46, 47
iSCSI 26, 27, 44
iSNS 26

K

Kensington Lock 7

L

Licenses
For multiple snap servers 31
Third Party applications 43
Local Groups 28
Local Users 28
Login to Admin Tool 9

M

MacintoshOS
Launching Snap Server Manager 10
Version required to run Snap Server Manager 10
Mapping a Drive 16
Menu Bar 22

N

NDMP Server 43
Network
Connecting to 7
Settings 25
Network Browser (Macintosh) 13
Network LED 6
NFS, connecting with 13
Notification 42

O

Open Files 29
OS Update 30

P

Permissions, assigning 39
Phone Home Support 51
Power Button 6
Power Connector 7
Power LED 6
Power Off 8
Power On 8
Power Supply Retainer Clip 7
Print Server
Adding the Network Printer to the Client 46
Adding the Print Server to a Client Machine 46
Canceling Print Jobs 47
Configuring 45
Configuring the Printer on the Snap Server 45
Deleting a Printer from the Snap Server 48
IPP port number 46, 47
Monitoring Print Jobs 47
Pausing the Printer 47

Q

Quotas 27, 40

R

RAID 0 34, 35
RAID 1 35
RAID Sets 27
Recovery Image 30
Registration 13, 25
Reset Button 6
Restart Server 30
Retainer clip 7

S

Secure Shell 24
Security 49
  Accessing with guest privileges 41
  Assigning disk usage quotas 40
  Assigning user access 39
  Defining Snap Server users 37
Security Guides 28
Security Model
  Unix 28
  Windows 28
Server Name
  Configure 12
  Discovering 8
  Using to connect to the network 9
Server Registration 13
Server Settings 24
  Modifying 33
Service Port 7
Setup wizard, see Initial Setup Wizard
Shared Folders 39
Shares 27, 28
Shares, creating 36
Shut Down 8, 30
Snap EDR Agent 43
Snap Finder 23
Snap Server
  Connecting to 8
  Customizing 33
  Locating on Network 13
Snap Server Manager 43
  Installing 10
  Launching 10
  Supported Platforms 10
  Using to connect to the network 10
  Using to license multiple snap servers 31
  Using to manage multiple Snap Servers 32
Snap Server Web site 49
SnapExtensions 23, 43
Snapshot Space 12, 34
Snapshots 44
  Scheduling 27, 44
SnapTrees 28
SNMP Agent 26
SSH 24
Static IP Address 25
Status LED 6
Storage Guides 27
Subnet Mask 11
Support 29, 51
System Configuration 29
System Status 29

T

Technical Support Telephone Numbers 3

U

Unicode 25
Unix File Security 49
Update GuardianOS 30
UPS 8, 24
USB Ports 7
User Information 29
Users
Access to files and folders 39
Access to network shares 39
Accessing as guest 41
Defining 37
Local Users 38
Network 38
Pre-defined 37
Usage quotas 40
Windows domain security 38

V

Volumes 27
Usage 29

W

Web Browser, connecting with 13
Web View 9
Windows 26, 28